„Der in der Eröffnung [...] angesprochene Topos der Verschwörungstheorie sei [...] bereits in der Vorbereitung im Bewusstsein gewesen, sodass der Vortrag darauf ausgerichtet worden sei, keine Verschwörungstheorien zu entwickeln oder zu bedienen. Es ergebe sich jedoch die Frage, ob im aktuellen gesellschaftlichen Diskurs überhaupt noch außerhalb von Verschwörungstheorien gedacht werden könne.“ (Florian Wobser u. Tom Gehrke, S. 44)

„Die aktuelle Lage zwinge förmlich zum Bild einer Gesellschaft unter Generalverdacht, in der jedes Individuum dem Vorwurf unterliege, etwas zu verbergen zu haben, da anders der status quo einer anlasslosen Massenüberwachung nicht zu erklären sei.“ (Dr. Anne Käfer, S. 98)

„Es sei in der Tat ein falscher Weg, den Staat zu dämonisieren und pauschal zu behaupten, dieser greife gegen Überwachung nicht ein. […] Dagegen sei anderen staatlichen Institutionen der zuvor erwähnte Schutzgedanke für Bürger_innen kaum anzurechnen. [...] Der ehemalige Bundesminister des Innern Manfred Kanther habe bspw. einmal auf einem Kongress gesagt, man habe seit hundert Jahren die Möglichkeit abzuhören und wolle deswegen auch keine Kryptographie haben, damit man weiter abhören könne.“
(Prof. Dr. Ernst-Günter Giessmann, S. 68)

„Der kommerzielle Wert von Informationen und Daten sei zu vergleichen mit dem von Gold [...]. Die Politik wisse um den Wert derartiger Datenbestände über die Bevölkerung, da sich mit genauen Informationen über die Bevölkerung bspw. ein Wahlkampf bis in einzelne Straßenzüge hinein so individualisieren ließe, dass ein Popularitätsgewinn für die jew. Partei garantiert sei. Unter dem Ideal einer Demokratie aus Individuen, die diese ausgestalteten, stimme eine solche Zukunftsaussicht pessimistisch.“ (Doris Aschenbrenner, S. 90)

„Unter wirtschaftlicher Betrachtung sei das Internet ebenso in nationale Märkte aufgeteilt. Entsprechend stelle sich die Frage, warum nationale Datenschutzregelungen der realen Welt nicht auch für die virtuelle als Kriterium herangezogen werden könnten, wolle ein Unternehmen eine virtuelle Dienstleistung bspw. auf dem deutschen Markt anbieten.“ (Michaela Zinke, S. 45)

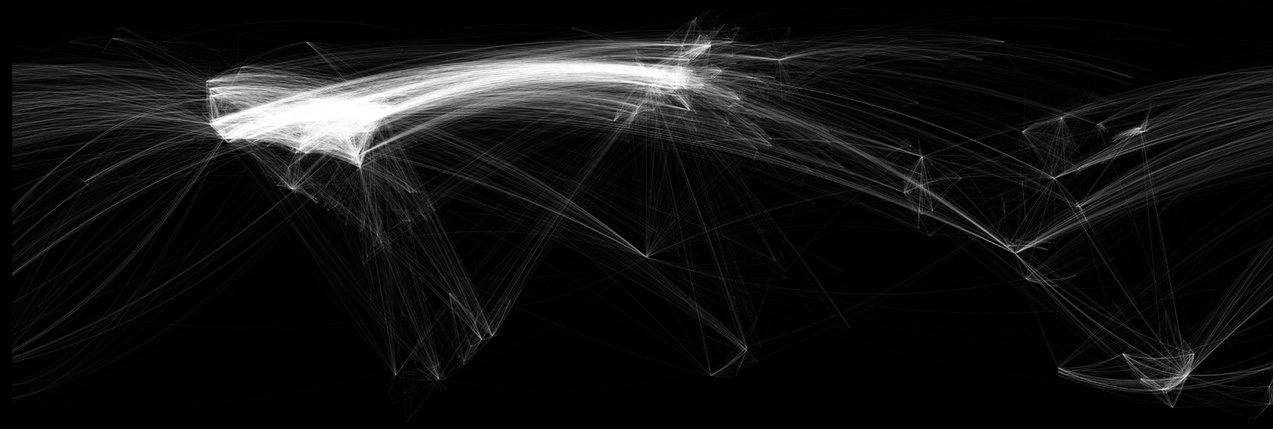
„Bürger_innen könnten sich in der Überwachungsthematik nicht auf politische Parteien verlassen. […] Wichtig sei, sich beständig zu informieren, aktiv zu werden und anzufangen, sich selbst im digitalen Raum zu schützen.“ (Nele Trenner, S. 92)

„Das Desinteresse an sich etablierenden totalitären gesellschaftlichen Strukturen sei vergleichbar mit dem Desinteresse, für einen Service oder eine Software Geld zu zahlen, welches wiederum Ausdruck einer Bequemlichkeitshaltung sei, die erstens alles für eine kostenlose Smartphone-Applikation opfere, was vorangegangene Generationen gesellschaftlich hart erkämpft hätten, und zweitens sich so der Verantwortung zum Erhalt schwer erkämpfter Freiheitsrechte entziehe.“ (Leena Simon, S. 61)

„Das erste ist Trauer, das zweite ist Ratlosigkeit und das dritte ist das aktive Vertrauen darauf, daß unsere Werte stärker und überzeugender sein werden, wenn wir denn entschlossen und konsequent wirklich an ihnen festhalten.“ (Friedrich Schorlemmer, S. 8)

Online-Ausgabe

HUMBOLDT-UNIVERSITÄT ZU BERLIN



Jahr 1 nach Snowden

Eine studentische Initiative an der HU-Berlin zur Kontroverse der globalen Überwachungsaffäre

Sammelband zur interdisziplinären studentischen Initiative
„Edward – der Whistleblower, der nichts enthüllt hat?
Zum Vorwurf des „Digitalen Analphabetismus“ im Jahr 1 nach Snowden“
an der HU-Berlin im WiSe 2014/15 mit Beiträgen von:

Florian Wobser, Tom Gehrke, Michaela Zinke,
Leena Simon, Prof. Dr. Ernst-Günter Giessmann,
Doris Aschenbrenner, Dr. Anne Käfer, Nele Trenner
und Friedrich Schorlemmer

In Kooperation mit dem Deutschen Journalistenverband Berlin e.V. und der FIfF-Konferenz 2014
Initiatoren und Herausgeber: Amon Kaufmann und Roland Hummel

Online-Ausgabe

Bildnachweise:
Umschlag, Vorderseite: "Internet Map city-to-city connections" mit freundlicher Genehmigung von Chris Harrison, www.chrisharrison.net/
Umschlag, Rückseite:
Profilbild F. Schorlemmer: Michael Reichel
Profilbild L. Simon: Alexander Altmann
(übrige Profilbilder mit freundlicher Genehmigung der Gastredner_innen)
Gestaltung des Einbandes: Sunah Yu
Kontakt der Herausgeber:
Amon Kaufmann (kaufmann@physik.hu-berlin.de) | Roland Hummel (roland.hummel@theologie.hu-berlin.de)

Jahr 1 nach Snowden

Eine studentische Initiative an der HU-Berlin zur Kontroverse der globalen Überwachungsaffäre

Sammelband zur interdisziplinären studentischen Initiative
„Edward – der Whistleblower, der nichts enthüllt hat?
Zum Vorwurf des „Digitalen Analphabetismus" im Jahr 1 nach Snowden“
an der HU-Berlin im WiSe 2014/15 mit Beiträgen von:

Florian Wobser, Tom Gehrke, Michaela Zinke,
Leena Simon, Prof. Dr. Ernst-Günter Giessmann,
Doris Aschenbrenner, Dr. Anne Käfer, Nele Trenner
und Friedrich Schorlemmer

Initiatoren: Amon Kaufmann und Roland Hummel

Herausgeber: Roland Hummel

Unterstützt vom Studierendenrat der Theologischen Fakultät und dem StudentInnenparlament der Humboldt-Universität zu Berlin sowie dem Allgemeinen Studierendenausschuss der FU Berlin.

In Kooperation mit dem Deutschen Journalistenverband Berlin e.V. sowie der FIfF-Konferenz 2014.

Bearbeitungsstand vom 23. Jun. 2017 (Online-Ausgabe in zweiter Version unter Creative Commons)

Erstausgabe (Bearbeitungsstand vom 18. Nov. 2015) gedruckt durch die Druckerei der

Humboldt-Universität zu Berlin (Auflage: 200 Bände)

1 1

2 Für Amon

1 Bildnachweis: A. Kaufmann 03. Nov. 2014 © Sunah Yu.

Inhaltsverzeichnis

Geleitwort von Friedrich Schorlemmer

„Für den Verrat unwürdiger Geheimnisse“ – Eine Hommage auf Edward Snowden

Friedrich Schorlemmer 16.11.2015

Edward Snowden wollte seinem Land dienen und mit seinen entlarvenden Aktionen den Werten seines Landes genüge tun. Sein Wissen rieb sich an seinem Gewissen und so machte er welt-öffentlich, was sich die NSA weltweit herausnimmt. Die angemaßte Weltpolizei USA mit ihren globalen Überwachungs- und Bestechungsnetzen fühlte sich entblößt. Wer ans Licht bringt, was finster ist, was „faul ist im Staate Dänemark“, wird alsbald als Verräter verfolgt, bis der, der Bestürzendes ans Tageslicht gebracht hat, was im Dunkeln bleiben sollte, selber in ein finsteres Verlies verbracht werden kann, mundtot gemacht werden soll und nun ausgerechnet im Russland Putins Zuflucht suchen und notgedrungen finden konnte, wodurch sich die Propaganda Russlands bestätigt und salviert vorkommen konnte und kann. Die Geheimdienste der Welt unterscheiden sich nur graduell, kaum prinzipiell. So gab es geheime Zwangsinternierungslager in Ländern, wo bestimmte „verschärfte“ Folterpraktiken nicht ausdrücklich untersagt sind und somit nicht verfolgt werden. Geheimdienste unterlaufen rechtsstaatliche Prinzipien, um an ihre Informationen heranzukommen.

Das gilt als ethisch vertretbar, weil auf diese Weise Schlimmeres verhütet würde. So betrieben sie eine grenzenlose, jedes Recht unterlaufende Verbrechenspräventivstrategie, die geheim bleiben musste, wenn sie gelingen sollte. Wer verrät, welcher Methoden sich insbesondere die Führungsmacht durch Abhören unter Freunden leistete – bis hin zur Bundeskanzlerin – wird wie ein Krimineller behandelt, obwohl er nur Kriminelles aufgedeckt hat. „Abhören unter Freunden, das geht gar nicht“, hatte die Kanzlerin 2013 noch empört geäußert, bis sich nun herausstellt, daß der BND, nicht bloß die NSA/CIA, Informationen zuliefert oder von deren Informationen profitiert, sondern auch selber – außerhalb politischer oder parlamentarischer Kontrolle – den französischen Außenminister oder gar eigene höhere Diplomaten abhört. Wusste die Bundeskanzlerin nicht was der BND gemacht hatte oder wurde selbst ihr gegenüber das „geheim gehalten“?

Der Dokumentarfilm über Edward Snowden mit dem Titel „Citizenfour“ wurde von der Leipziger Stiftung „Friedliche Revolution“, in dessen Kuratorium ich tätig bin, mit dem Dokumentarfilmpreis „Leipziger Ring“ ausgezeichnet. Es lag uns daran, heutigen Wahrheitsmut zu würdigen. Der Film gewann weitere Preise, aber Snowdon sitzt immer noch in Russland fest. Er hat die rechtsstaatlichen Prinzipien seines eigenen Landes hochgehalten und die politisch-moralische Selbstdemontage der USA offengelegt. Nun wird diesem als Verrat zugerechnet, was er an Verrat aufgedeckt hat! Die Demokratie braucht solche Menschen, die ohne irgendeinen Vorteil, gar mit einem schweren Nachteil rechnend, aufklären. Die Staatsräson zu befolgen darf nicht heißen, daß man schweigt, wo offen-gelegt werden muss.

„Für den Verrat unwürdiger Geheimnisse“ wollte Ingeborg Bachmann einen Preis verliehen sehen: „die Auszeichnung der armselige Stern der Hoffnung über dem Herzen… für die Tapferkeit vor dem Freund.“

Snowden ist ein einsamer Held unserer Tage und ist glücklicherweise nicht allein geblieben, findet wache Geister der Demokratie überall auf der Welt.

Dieser Dokumentationsband ist Resultat eines wachen Gewissens und notwendigen Wissens über das, was zur Debatte steht: unser aller Freiheit, unser aller Schutz vor Geheimdiensten, die angeben, uns schützen zu müssen und dabei technisch ausgeklügelte Weise jederzeit bei jedermann alles geheim dokumentieren können. Dabei sollte freilich außer Frage stehen, daß Geheim-Dienst-Wissen notwendig sein kann, wann und wo menschliches Leben durch Terrorstaaten oder zivilisierte Terroristen gefährdet oder somit Gefahr abgewehrt wird. Da bleiben Grauzonen. Klar bleiben muss, dass die Prinzipien, die man punktuell außer Kraft zu setzen genötigt zu sein behauptet, generell gelten und Priorität behalten.
Welch eine Ineffizienz haben diese aufwändigen und teuren Geheimdienste weltweit? Warum zum Beispiel wusste man erst von ISIS und IS als er schon seine mörderische Praxis auf erschütternde Weise – medial zynisch begleitet – entfaltet hatte? Wo waren unsere deutschen Geheimdienste in zehn Jahren der sogenannten „Dönermorde“? Warum haben sie bewusst nur inner-islamisch gesucht und sind einer einzigen – falschen – Spur gefolgt? Was ist mit dem Völkerrecht, wenn weltweit Drohnen alles unter ihre Kontrolle und auch unter ihre Tötungsmacht nehmen dürfen? Welche Rolle spielten (westliche) Geheimdienste in der Ukraine beim Sturz von Janukowitsch? Welche (absehbaren) Folgen hatte der im Westen so begrüßte und unterstützte „Arabische Frühling“? Sollte nun endlich der von Bush Jr. erwartete demokratische Dominoeffekt eintreten, den er bei seinem durch Lügen vor der UN vorgetragenen, aber nicht legitimierten Krieg vorausgesagt hatte? Wieso konnten vier Flugzeuge in einer konzertierten Aktion terroristisch in amerikanische Lebenszentren eindringen, so viele Opfer kosten und einen „New War“ auslösen?
Was wussten Geheimdienste über die mörderische Regenerationskraft der Taliban – ohne Mullah Omar und den mysteriösen Bin Laden, dessen Hinrichtung per Satellit die amerikanische Regierung beiwohnte? Selbst Präsident Obama scheint es wichtiger zu sein, den Überbringer der enthüllenden Nachrichten zu fassen und anzuklagen, als aufklärend zu enthüllen, welch ein demokratiegefährdendes Mammutpotential in den NSA-Praktiken steckt und stattdessen diejenigen zu fassen und zu disziplinieren, die den Ruf der „Weltmacht der Freiheit“ ruinieren.
Was wird schließlich, wenn keiner keinem mehr trauen kann? Dann herrscht das Prinzip Misstrauen. Tunlichst ist zu vermeiden, seine Werte so zu verteidigen, dass diese von innen in Misskredit kommen, ja jede Glaubwürdigkeit einbüßen. Ein redlicher Verteidiger der Werte muss sie so verteidigen, dass erkennbar und erfahrbar bleibt, dass die Wege zum Ziel passen. Nur in extremen Fällen werden auch Geheimdienste Gewalt einzusetzen genötigt sein. Indes: auf den Wegen zum Ziel muss das Ziel so unbeschadet wie möglich bleiben.
Mit diesem Dokumentationsband leisten engagierte Studenten mit Vertretern der Zivilgesellschaft in Deutschland ihren Beitrag nicht nur zur Verteidigung von Edward Snowden, sondern sie lassen auch erkennen, welch einen Mut dieser einzelne Mann hatte und zu welchem Mut er uns in der Demokratie herausfordert – so lange wir noch Demokratie, Datenschutz, informationelle Selbstbestimmung

einfordern können, verbunden mit der Kontrolle der (international agierenden) unersättlichen Geheimdienste.
Nach den grausigen Terrorakten am Freitag, dem 13. November in Paris – und zuvor in Beirut und in Ankara! – steht unser aller Freiheit zur Debatte. Es sind nicht Verbrechen *des* Islam, sondern Verbrechen *gegen* den Islam. Gewinner in der westlichen Hemisphäre sind jetzt wieder die Geheimdienste – ob deren Aufstockung und ihre Kompetenzerweiterung wirklich hilft oder nicht.

Die NZZ fordert offen das militärische Engagement Deutschlands in den Wüsten des Irak und Syriens. Gnade uns allen!
Aber wie des gnadenlos mordenden IS Herr werden, damit Auseinandersetzung wieder zivilisiert ablaufen? In die Trauer mischt sich viel Ratlosigkeit. Wo werden wir uns wiederfinden?
Die Weltzivilisation steht zur Debatte seit dem 11. Sep. 2001. Wie reagieren? Mit einem neuen Krieg? Muss man nicht zunächst fragen, was den Terrorismus befeuert hat? Der Krieg! Der erlogene Krieg im Irak und der vierzehn Jahre dauernde, im Ganzen vergebliche Krieg gegen die Taliban in Afghanistan.
Das ist ein barbarischer Angriff auf die Menschlichkeit, die menschliche Zivilisation, auf die Freiheit, auf die Menschenrechte, auf unsere Lebensweise und nicht zuletzt auf den Islam. Die Flüchtlingsströme setzen sich aus Menschen aus der arabischen Welt zusammen, die vor dem IS fliehen und nicht aus solchen, die den mörderischen IS zu uns bringen wollen. Aber sie könnten sich darunter mischen wollen.
Aber bitte die Flüchtlinge nicht unter der Hand in Generalverdacht bringen!

Wer *Paris* Freitag, den 13.November sagt, muss auch *Ankara*, 10. Oktober und *Beirut*, 12. November sagen. Tragische Opfer an allen drei Orten sind unterschiedslos Menschen, die zufällig am falschen Fleck waren. Es gibt keine Kombattanten mehr. Es gibt nur hasserfüllten, lebensverachtenden, unterschiedslos zuschlagenden Terror.

Diesen mörderischen Zynismus zu beschreiben fehlen mir die Worte.
Das erste ist Trauer, das zweite ist Ratlosigkeit und das dritte ist das aktive Vertrauen darauf, daß unsere Werte stärker und überzeugender sein werden, wenn wir denn entschlossen und konsequent wirklich an ihnen festhalten.

Im Übrigen würde es der Bundesrepublik Deutschland zur Ehre gereichen, wenn Edward Snowden in unserem Land dauerhafte Zuflucht fände, ohne, dass das als Affront gegen die USA gemeint oder benutzt wird, sondern als Signal: Geheimdienste bedürfen überall der Kontrolle – zunächst unserer eigenen. Und die Artikel 10 und 13 des Grundgesetzes bedürfen neuer Ausführungsbestimmungen, die den heutigen technischen Möglichkeiten ebenso Rechnung tragen, wie eine größere Gewähr dafür zu schaffen ist, dass künftigen Missbräuchen beim Ausforschen entgegengewirkt wird.

Die gigantischen Ausmaße des neuen BND-Gebäudes in Berlin lassen nicht gerade das Vertrauen wachsen, daß der BND seine Befugnisse einschränken könnte.

Die Demokratie bedarf auch ihres wehrhaften Schutzes (auch im Hintergrund), aber noch viel mehr der wahrnehmbaren und wahrgenommenen Freiheits- und Entfaltungsrechte des Einzelnen auf der Grundlage der universellen Menschenrechte.

Vorwort der Initiatoren

Aus einem abendlichen Spielfilm: Ein durchtrainierter Mann in adrettem Anzug kopiert in geheimer Mission an einem Regierungsrechner einer mächtigen Industrienation hoch vertrauliche Dokumente. Er bemerkt Schritte aus dem Korridor, wartet souverän die letzten Sekunden des Kopiervorgangs ab, rückt sich die Fliege zurecht und verschwindet mit den Daten in einem Lüftungsschacht. Der Großalarm lässt nicht lange auf sich warten. Der unerwünschte Geheimnisträger übergibt die kopierten Daten bei einem geheimen Treffen der Presse, die dadurch kurze Zeit später den größten Überwachungsskandal der Geschichte aufdeckt, welcher umgehend von einem Regierungsvertreter mit Vehemenz dementiert wird. Die Regierungsbeamten immer dicht im Rückspiegel, flieht der Enthüller, für die Staatsmacht ein Verräter, für das Volk ein Held, um den halben Erdball von einer Action-Szene in die nächste, nur unterbrochen von unterhaltsamen Sprüchen, sobald ihn Passanten aufgrund der unablässigen Berichterstattung wiedererkennen. Diplomatische Kollateralschäden lassen nicht lange auf sich warten: Der Präsident eines unbeteiligten Entwicklungslandes wird, nachdem dieser während einer Auslandsreise beiläufig seine Sympathie für den Flüchtigen zum Ausdruck brachte, auf dem Rückweg in sein Heimatland über fremdem Territorium zur Landung gezwungen. Der Verdacht: im Bauch des Flugzeuges könnte sich der weltweit gesuchte Protagonist befinden! Der Cliffhanger folgt im Transitbereich des internationalen Flughafens eines Landes, das eigentlich nur Zwischenstation im Plan des Verfolgten sein sollte. Schließlich bleibt ihm, einen Prozess wegen Landesverrats mit mindestens lebenslanger Haft vor Augen, nur der Ausweg, nun an seinem unverhofften Aufenthaltsort um Asyl zu bitten – ausgerechnet in einem Land, welches sich laut der Allianz der nunmehr entlarvten Überwachungsstaaten einen festen Platz in der „Liga der ewigen Schurkenstaaten“ verdient hat...

Entfernen wir nun aus dieser „Traumfabrik“ die Bond-Anzüge, die Action-Sequenzen, die Verfolgungsjagden und die Heldensprüche, so dämmert es langsam: das ist ja gar kein Film, sondern die Realität, die sich, je länger man sie betrachtet, vielfach diversen „1984“-Dystopien zu bedienen scheint. „DER GROSSE BRUDER SIEHT DICH“[2] tatsächlich. Nur die Konsquenzen, oder genauer gesagt: die „Ministerien für Frieden, Liebe, Wahrheit und Überfülle“, die „Hasswochen“, die überwachenden, nicht abschaltbaren „Teleschirme“, die alternativlose „Krieg ist Frieden“-Politik, schließlich die „Unpersonen“, die fehlen doch – oder?

Wir hoffen, dass die nachfolgenden Themen zur Kontroverse der globalen Überwachungsaffäre, die wir in diesem Sammelband der stud. Initiative „Jahr 1 nach Snowden“ versucht haben unter verschiedenen Perspektiven einzufangen, Sie zum Protest einladen werden – sowohl für als auch gegen alle dabei entwickelten Gedanken. Möge Ihnen zu diesem Zweck der vorliegende Sammelband sowohl eine hilfreiche „Expeditionslektüre“ als auch eine „Machete“ im Unterholz westlicher Politik sein.

Amon Kaufmann und Roland Hummel

2 So die deutsche Übersetzung des Originals in: ORWELL, G.: „1984“, übersetzt von M. Walter, Ullstein Buchverlage GmbH, Berlin [31]2007, 8.

Es ist den Initiatoren leider unmöglich, all den vielen Helfer_innen gebührend zu danken, die uns in den Vorbereitungen der stud. Initiative ab Mai 2014 immer wieder darin unterstützten, das „Jahr 1 nach Snowden“ so umfangreich zu diskutieren. Ihnen allen möchten die Initiatoren an dieser Stelle **Danke** sagen, im Besonderen:

Doris Aschenbrenner,
Karsten Asshauer und dem CMS der HU-Berlin,
Alexander Czekalla und dem DJV Berlin,
Ilse Dänecke,
Tom Gehrke,
Prof. Dr. Ernst-Günter Giessmann,
Dr. Anne Käfer,
Anne Lorenz und dem Team der Uni-Druckerei der HU-Berlin,
Kai Lüke und dem AStA-FU Berlin,
Rainer Rehak und dem FifF,
Katie Anne Revell,
Janna Marie Röwer,
Friedrich Schorlemmer,
Prof. Dr. Jens Schröter,
Leena Simon,
der Stabsstelle Presse- und Öffentlichkeitsarbeit der HU-Berlin,
dem Studierendenrat der Theologischen Fakultät der HU Berlin,
Robert Stöber,
Nele Trenner,
Moritz Wiederänders,
Florian Wobser,
Maren Wissemann,
Sunah Yu
und Michaela Zinke

Zum Anliegen der studentischen Initiative

Im Zuge der Aufdeckung der weltweiten Überwachungs- und Spionageaffäre durch die im Juni 2013 an die Presse gesandten Dokumente des Whistleblowers Edward Snowden beobachten die Initiatoren der „Jahr 1 nach Snowden“-Initiative intensiv die gesellschaftspolitischen Auseinandersetzungen mit diesen Enthüllungen sowie die mit ihnen verbundenen kontroversen Reaktionen in Deutschland. Über die Feststellung hinausgehend, dass der gesellschaftliche Tenor zwar mehrheitlich durch Empörung geprägt, jedoch mit Konsequenzen privater wie öffentlicher Art eher zurückhaltend war, fanden die Initiatoren es bedenklich, dass eine Auseinandersetzung mit diesem vielschichtigen Thema, welches von globalerer Dimension kaum sein könnte, an den Universitäten, von einigen wenigen Ausnahmen ideeller Würdigung abgesehen, bis zum Start der Initiative Anfang November 2014 kaum vorhanden war. Bedenklich ist dieser Umstand, weil es Universitäten waren, welche an der Idee einer weltweiten Vernetzung durch das Internet und seiner Vorläufer seit den 70er Jahren maßgebend mitwirkten. Damit sehen die Initiatoren die Universitäten in einer Verpflichtung, am Erhalt einer sehr gefährdeten „Netzkultur“ und „Netiquette“ mitzuwirken.

Die Kultur des Internets wie auch die mit ihr verbundenen Umgangsformen des 21. Jh. lassen sich nach Meinung der Initiatoren von ihren Pendants des nicht-virtuellen Raumes kaum trennen. Die Enthüllungen im Zuge der Überwachungs- und Spionageaffäre ermöglichen es in diesem Zusammenhang, auf einer neuen Ebene über die Gefährdung der allgemeinen Kultur wie auch der Netzkultur zu diskutieren. Die Initiatoren wollten diese Diskussion unter möglichst vielfältigen Gesichtspunkten als Teil des wissenschaftlichen Diskurses an der Humboldt-Universität führen. Der Leitspruch der Humboldt-Universität - „Bildung durch Wissenschaft“ - sollte auch in diesem Zusammenhang dem Anspruch gerecht werden, Interessierten aus allen Teilen der Gesellschaft die Möglichkeit zu geben, sich in der vorfindlichen Komplexität der Ereignisse durch sachliche Auseinandersetzung fundierter positionieren zu können. An der folgenreichen Überwachung des HU-Soziologen Andrej Holm, die in dessen unbegründeter Verhaftung im Jahr 2007 endete, wird deutlich, wie dringend ein aktiver Schutz vor Überwachung an Universitäten erfolgen sollte.

Der ursprüngliche Titel der Initiative („Edward - der Whistleblower, der nichts enthüllt hat? Zum Vorwurf des 'Digitalen Analphabetismus' im Jahr 1 nach Snowden“) bezog sich inhaltlich auf zwei Beiträge der Debatte: zum einen „Whistleblower Edward Snowden - Der hat doch gar nichts enthüllt“ (Wolfgang Michal, 10.06.2014, Frankfurter Allgemeine Zeitung / Feuilleton), zum anderen „Estland - Präsident Ilves und die Digitalisierung seines Landes“ (Gabor Paal, 18.12.2013, Deutschlandfunk / Europa heute). Die Beiträge kommentierten das Thema in provokanter Weise, da sie zugleich die Bedeutung der Überwachungsaffäre in Frage stellten als auch die innerdeutsche Kompetenz, sich mit ihr auseinandersetzen zu können. Diesem Spannungsfeld wollten sich die Initiatoren mit einer öffentlichen Veranstaltungsreihe aus drei Themenblöcken nähern, die sowohl theoretisch (durch Diskussion) als auch praktisch (am Computer) die eigene Position im Umgang mit der Überwachungsaffäre nachhaltig schärfen sollten. Abschließend möchten die Initiatoren auf den „Ideenkatalog zum Umgang mit der Überwachungsaffäre“ am Ende des Sammelbandes hinweisen, der in diesem Fall der HU-Berlin

gewidmet ist, aber inhaltlich auch andere Bildungseinrichtungen oder Unternehmen darin unterstützen möchte, zum Schutz von Forschung (und Lehre) der globalen Überwachungsaffäre zu begegnen.

Allgemeine Hinweise

Projektseite der Initiative

Die offizielle Projektseite der Initiative ist abrufbar unter:
http://jahr1nachsnowden.de/ (zuletzt aufgerufen: 01. Nov. 2015)
Diese Projektseite wird min. bis Okt. 2016 von den Initiatoren finanziert. Anschließend werden die Inhalte nach derzeitiger Planung in den nachfolgend erwähnten Moodle-Kurs überführt.

Moodle-Kurs der Initiative

Die Ergebnisse der Initiative sind in digitaler Form in einem vom Computer- und Medienservice der Humboldt-Universität zu Berlin bereitgestellten Moodle-Kurs abrufbar:
https://moodle.hu-berlin.de/course/view.php?id=60669 (zuletzt aufgerufen: 28. Apr. 2017)
Kurzlink: https://hu.berlin/jahr1nachsnowden
Der Moodle-Kurs ist akt. ohne Anmeldung abrufbar.

Wiki-Themenportal „Überwachungsaffäre“

Mit Unterstützung des Computer- und Medienservice der Humboldt-Universität zu Berlin wird im Wiki der HU-Berlin ein Bereich zum Thema „Überwachungsaffäre“ gepflegt:
https://wikis.hu-berlin.de/dvb/%C3%9Cberwachungsaff%C3%A4re (zuletzt aufgerufen: 28. Apr. 2017)
Kurzlink: https://hu.berlin/ueberwachungsaffaere
Das Wiki ist öffentlich, für die Mitarbeit am Wiki wird akt. ein HU-Account benötigt.

Zu den Protokollen der Theorieveranstaltungen

Die Inhalte der Protokolle wurden mit Genehmigung der jew. Gastredner_innen gedruckt.
Die in den Vorträgen erwähnten englischsprachigen Beiträge hat der Protokollant zum besseren Verständnis des Gedankenganges für nicht-englischsprachige Leser_innen übersetzt und in längeren Übersetzungen für Englischkundige jeweils die seiner Ansicht nach zentralen Passagen der englischsprachigen Quelle in eckigen Klammern zur Orientierung eingefügt.
Hinweis zu den Fußnoten: Unkommentierte Fußnoten verweisen auf Erklärungshilfen in der Veranstaltung genannter Begriffe oder Abkürzungen. Mit „Vgl.“ kommentierte Fußnoten verweisen auf weiterführende Informationen in der Veranstaltung angesprochener Themen. Mit „Anm. d. Pr.: Vgl.“ kommentierte Fußnoten verweisen auf weiterführende Informationen zu Themen, die auf der Veranstaltung nicht direkt angesprochen worden, aber nach Meinung des Protokollanten im Zusammenhang von Interesse sein könnten.

Zu den Entwürfen der Praxisveranstaltungen

Die in diesem Sammelband präsentierten Entwürfe waren Grundlage dreier Praxisveranstaltungen, die als möglichst einsteigerfreundliches Programm an Wissbegierige gerichtet waren, die bisher in den Bereichen "Datenanalyse", "Verschlüsselung" und "Datensicherheit" keine oder nur sehr geringe Vorkenntnisse besaßen, sodass in der Konzeption auf spezielle Vorkenntnisse bewusst verzichtet

wurde, um das Programm einer möglichst breiten Öffentlichkeit zugänglich zu machen. In allen drei Praxisveranstaltungen überstieg die Zahl der Teilnehmer_innen (von Schüler_innen bis zu Rentner_innen) die vorhandenen Plätze deutlich, welches als Bestätigung für das hohe Interesse an Weiterbildungsmaßnahmen in den genannten Bereichen gesehen werden sollte. Die Entwürfe spiegeln inhaltlich den (besonders flüchtigen) technischen Stand ihrer Zeit wider und sollen daher nur als Ideengeber dienen, ähnliche Veranstaltungen zu konzipieren.

Zur Online-Ausgabe

Für den edoc-Publikationsserver[3] der Humboldt-Universität wurde im Dez. 2015 nach Veröffentlichung der Druckversion eine Online-Ausgabe bereitgestellt, bei der leider versäumt wurde, alle Inhalte, die dies erlauben, unter eine freie Lizenz zu stellen. 2017 wurde dies nachgeholt, sodass die vorliegende Ausgabe unter CC-BY-SA die folgenden Rechte *für alle Inhalte, die von Roland Hummel erstellt wurden,* gewährt:

Sie dürfen:

Teilen — das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten

Bearbeiten — das Material remixen, verändern und darauf aufbauen und zwar für beliebige Zwecke, sogar kommerziell.

Diese Lizenz ist geeignet für freie kulturelle Werke.

Der Lizenzgeber kann diese Freiheiten nicht widerrufen solange Sie sich an die Lizenzbedingungen halten.

Unter folgenden Bedingungen:

Namensnennung — Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.

Weitergabe unter gleichen Bedingungen — Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.

Keine weiteren Einschränkungen — Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Bezügllich der Texte sind dies alle bis auf das Geleitwort von F. Schorlemme sowie die Anhänge 2 und 3 von F. Wobser und T. Gehrke.

Da Amon Kaufmann 2017 verstarb führt die 2017er Online-Ausgabe als Herausgeber lediglich Roland Hummel.

3 http://edoc.hu-berlin.de/ (zuletzt aufgerufen: 28. Apr. 2017).

Studentische Initiative:
„Edward - der Whistleblower, der nichts enthüllt hat?
Zum Vorwurf des "Digitalen Analphabetismus" im Jahr 1 nach Snowden“
Theorieveranstaltung I – „Vom Sinn des Privaten“ (03. Nov. 2014 – WiSe 2014/15)

Protokoll zur Auftaktveranstaltung „Vom Sinn des Privaten“

Gastredner_innen:	Michaela Zinke (MZ)
	Florian Wobser (FW)
	Tom Gehrke (TG)
Moderation:	Amon Kaufmann (AK)
Eröffnung und Protokoll:	Roland Hummel (RH)

Initiatoren:	Amon Kaufmann (kaufmann@physik.hu-berlin.de)
	Roland Hummel (roland.hummel@theologie.hu-berlin.de)

Eröffnung

Visualisierungen des Internetverkehrs aus den Jahren 2007 und 2011, erstellt durch den US-amerikanischen Informatiker und Künstler Chris Harrison, zeigten deutlich die Wandlung der digitalen Vernetzung in den vergangenen Jahren.[4] Das Jahr 2007 könne dabei exemplarisch für die Vernetzung durch das Web 2.0 gesehen werden, welches trotz einer gewissen Dominanz der Verbindungen zwischen Europa und den USA den Globus insgesamt erschlossen habe und Nutzer_innen die Vorzüge globaler Kommunikation erfahren lassen habe (Folie 2)[5]. Im klaren Kontrast dazu stehe die Visualisierung aus dem Jahr 2011 (Folie 3), deren Verbindungen die Kontinente nicht nur durchzögen, sondern die Welt gänzlich dominierten und gleich einem digitalen Äther umhüllten. Befürchtungen eines Missbrauchs dieser allumfassenden Vernetzung gehörten jedoch 2011 allgemein in die Kategorie der Verschwörungstheorien. Erst die Enthüllungen durch den ehemaligen US-amerikanischen Geheimdienstmitarbeiter Edward Snowden konnten erstmals stichhaltig den Nachweis der Umwandlung des Internets in eine globale Überwachungsmaschinerie erbringen. Relikte dieser Maschinerie fänden sich auch in Berlin. Die verlassenen Gebäude der ehemaligen Abhöranlage auf dem Berliner Teufelsberg (Folie 4) zeigten jedoch ein trügerisches Bild, da mittlerweile klar sei, dass es aufgrund der allgegenwärtigen Vernetzung nicht mehr zwingend dieser Gebäude bedürfe, um in jeden Winkel der Privatsphäre vorzudringen wie es bspw. auf der „Freiheit statt Angst 2014“-Demonstration thematisiert worden sei (Folie 5).

Die stud. Initiative „Jahr 1 nach Snowden“ wolle einen Beitrag leisten, die gesellschaftspolitische Debatte zur Überwachungs- und Spionageaffäre mit voranzubringen und unternehme den Versuch, die mit ihr verbundenen Themen im wissenschaftlichen Diskurs der Humboldt-Universität zu Berlin zu erörtern. Die Notwendigkeit dafür ergebe sich aus der Beobachtung der gesellschaftspolitischen Debatte seit Beginn der Überwachungsaffäre. Dabei werde deutlich, dass sich diese Debatte im Hinblick auf die Komplexität der Ereignisse um den Kern einer kollektiven Ohnmacht sowie einer erlernten

4 http://www.chrisharrison.net/index.php/Visualizations/InternetMap (zuletzt aufgerufen: 02. Okt. 2015).

5 Angaben der Folien dieses Abschnitts s. Anhang 1 »„Vom Sinn des Privaten“ – Präsentationsfolien der Eröffnung«.

Machtlosigkeit bewege.[6] Extrema dieser Debatte flossen in den offiziellen Veranstaltungstitel[7] der Initiative mit ein. So sei zum einen die Behauptung aufgestellt worden, Edward Snowden habe im Grunde „gar nichts enthüllt“[8] sowie zum anderen von ausländischer Seite vorgeworfen, die innerdeutsche Diskussion bewege sich auf dem „Niveau digitaler Analphabeten“[9].

Grundlegend für folgende technische und gesellschaftspolitische Diskussionen solle die Auftaktveranstaltung „Vom Sinn des Privaten“ jenen Bereich untersuchen, der im Visier der globalen Überwachung stehe: Den Bereich der Privatsphäre. Anlässlich dieser Thematik habe die Initiative drei Gastredner_innen eingeladen, Impulse für eine Diskussion dieser Problematik zu liefern: Michaela Zinke aus Berlin sowie Florian Wobser und Tom Gehrke aus Rostock.

Vorstellung der Gastredner_innen

Tom Gehrke habe sein Abitur 2005 in Berlin abgelegt und 2007 ein Lehramtsstudium in den Fächern Sport und Geschichte aufgenommen. 2011 habe er seine Fächerkombination zu Philosophie und Geschichte hin gewechselt. Seine Studienschwerpunkte lägen in der Sozialphilosophie, Ethik und Phänomenologie.

Florian Wobser habe bis 2008 Lehramt für Gymnasium in den Fächern Philosophie und Deutsch an der Universität Rostock studiert und 2011 das Zweite Staatsexamen in Osnabrück abgelegt. Seit 2011 sei er Promotionsstudent und Lehrbeauftragter der Philosophie und ihrer Didaktik an der Universität Rostock. Sein Promotionsthema laute „Interviews und audiovisueller Essayismus Alexander Kluges - Ein ästhetisches Bildungsprojekt und seine didaktische Relevanz für schulisches Philosophieren“. Neben ersten Publikationen zum Promotionsthema und der Durchführung zahlreicher Seminare oblägen ihm Betreuungsaufgaben, Vorträge sowie die Durchführung von Fortbildungen für Referendar_innen und Lehrer_innen. Seine primären Forschungsschwerpunkte lägen in der kritischen Theorie zwischen Frankfurt und Frankreich, in der Medienphilosophie, der kritischen und ästhetisch-performativen Bildungstheorie, Essaytheorie sowie der Philosophiedidaktik.

Michaela Zinke sei Referentin für Datenschutz und Netzpolitik im Projekt "Verbraucherrechte in der digitalen Welt" des „Verbraucherzentrale Bundesverbandes“. Zielsetzung dieses Projektes sei die Befähigung von Bürger_innen, sich aktiv und sicher im Internet zu bewegen. Neben dem allgemeinen Spektrum ihrer Tätigkeit zum Datenschutz befasse sie sich speziell mit den Verhandlungen um die EU-Datenschutzverordnung und der juristischen Betrachtung konkreter datenschutzrechtlicher Problematiken von Internetdiensten. Ihr akademischer Hintergrund liege in einem Studium des

6 Vgl. MAAMAR, N., FIEDLER, L., MASCHKE, A.: „Zurück in die Zukunft – Wie Hochschulen mit den NSA-Enthüllungen umgehen“, UnAufgefordert 06/2014, 9.

7 Urspr. „Edward - der Whistleblower, der nichts enthüllt hat? Zum Vorwurf des "Digitalen Analphabetismus" im Jahr 1 nach Snowden“.

8 MICHAL, W.: „Whistleblower Edward Snowden - Der hat doch gar nichts enthüllt“, faz.net, 10. Jun. 2014, online abrufbar unter: http://www.faz.net/aktuell/feuilleton/whistleblower-edward-snowden-der-hat-doch-gar-nichts-enthuellt-12982298.html – Kurzlink: http://www.faz.net/-gqz-7q97e (zuletzt aufgerufen: 02. Okt. 2015).

9 PAAL, G.: „Estland - Präsident Ilves und die Digitalisierung seines Landes“, deutschlandfunk.de, 18. Dez. 2013, online abrufbar unter: http://www.deutschlandfunk.de/estland-praesident-ilves-und-die-digitalisierung-seines.795.de.html?dram:article_id=272407 – Kurzlink: http://kurzlink.de/Qjn7z5t8l (zuletzt aufgerufen: 02. Okt. 2015).

Wirtschaftsrechts an der HWR Berlin, ergänzt durch ein aktuell berufsbegleitendes Studium zum Informationsrecht an der Carl von Ossietzky Universität Oldenburg.

Gastvortrag von Florian Wobser und Tom Gehrke

Tom Gehrke wies einleitend darauf hin, dass sich Florian Wobser und er trotz punktueller akademischer Auseinandersetzungen zum Thema der Überwachungsaffäre nicht als Experten dieser Problematik sähen, sondern vor allem aus privatem Interesse und solidarischer Verbundenheit am Thema der Einladung an die Humboldt-Universität gefolgt seien. Ihr Gastvortrag gliedere sich in vier Bereiche (Folie 2)[10].

Zur Gliederung

Teil 1 befasse sich mit dem „heutigen Unsinn des Nicht-Privaten“, Teil 2 handle in historisch-systematischer Perspektive „vom einstigen Sinn des Öffentlichen“, Teil 3 setze sich daraufhin mit der Kritik an der klassisch-kant'schen Aufklärungsphilosophie aus Teil 2 auseinander und Teil 4 schließlich mit praktischen Beispielen, die Möglichkeiten aufzeigen würden, Grenzen zwischen „öffentlich“ und „privat“ in immer wieder neuer Weise zu setzen und zu verteidigen.

Teil 1 – Vom heutigen Unsinn des Nicht-Privaten

Zur optischen Veranschaulichung des ersten Abschnittes diene die „post-demokratische Merkel-Raute“ (Folie 3), deren Schema die inhaltlichen Pole der Problematik „Vom Sinn des Privaten“ ordnen solle: „Unfreiheit“ und „Freiheit“ als das erste sich gegenüberliegende Paar sowie „Transparenz“ und „Widerstand“ als das zweite (Folie 4). Transparenz habe dabei zwei Dimensionen (Folie 6): Zum einen die Bürger_innen auferlegte Transparenz im Bereich des Privaten, welche in ihrer extremsten Form zur Unfreiheit führe, zum anderen die von mündigen Bürger_innen eingeforderte Transparenz im Öffentlichen, die als Form des Widerstands einfacher einzufordern sei, während die im Bereich des Privaten nur mühsam zu vermeiden sei. Die sich daraus ergebende Frage sei, ob erstens Widerstand gegen Transparenz im Privaten möglich sei und zweitens, ob ein überwachter, transparenter Mensch noch ein freier Mensch sei (Folie 7).

Zur Verdeutlichung der heftig diskutierten Problematik über die Grenzen des privaten und öffentlichen Raumes folgte ein Ausschnitt aus der Diskussion der Berliner Konferenz „Einbruch der Dunkelheit“ vom Januar 2014 (Folie 8) mit dem IT-Sicherheitsexperten und Netzaktivisten Jacob Appelbaum sowie dem Politikwissenschaftler Christoph Bieber.

1.1 Exkurs „Einbruch der Dunkelheit“ - „Transparenz“ (J. Appelbaum, C. Bieber)

Appelbaum wandte auf die Erklärung Biebers ein, sein (Appelbaums) Soziales Netzwerk existiere nicht „auf der Straße“, weswegen klassischer Straßenprotest für Appelbaum keinesfalls die zuvor von Bieber beschriebene zentrale Bedeutung habe. Vielmehr habe sich der öffentliche Raum [„public sphere“] vor allem hinsichtlich der Kommunikation in das Internet verlagert.[11] Desweiteren würden besonders die vor

10 Angaben der Folien dieses Abschnitts s. Anhang 2 »„Vom Sinn des Privaten“ – Präsentationsfolien von Florian Wobser und Tom Gehrke“«.

Überwachung schützenden Systeme wie „Tor“[12] im aktuellen Ruf nach Abwehrmaßnahmen gegen Überwachung einen bedeutenden Beitrag leisten. Dies vor allem, weil es doch hauptsächlich darauf ankomme, Botschaften zu kommunizieren, welche eher zu Änderungen führten [„that helps things change quite a lot more in some cases“] als auf die Straße zu gehen und Fenster einzuschmeißen [„marching on the street and smashing a window“]. Straßenprotest sei nur eine Methode unter vielen für das Ziel der Übermittlung einer Botschaft, aber keinesfalls die wichtigste, um etwas zu bewegen [„disrupting things“]. Obgleich Berlin durch klassische Protestformen wie die der „Freiheit statt Angst“–Demonstrationen einen in der Welt überaus beeindruckenden Beitrag zum aktuellen Diskurs geleistet habe, sei doch der soziale und politische Wert [„social and political utility“] eines Snowden-Leaks ebenso wichtig und zwar ohne, dass Snowden dafür hätte auf die Straße gehen müssen. Der breiten öffentlichen Meinung, auf der Straße aktiv werden zu müssen [„to engage on the street“] könne Appelbaum nicht zustimmen – viel wichtiger sei es Geheimdienstdokumente durchsickern zu lassen [„that's weigh [?] more important: join the NSA and leak documents!“] als auf der Straße ignoriert oder gar erschossen zu werden. Bieber verteidigte daraufhin die Bedeutung des analogen Aktivismus [„analogue activism“] neben dem digitalen, denn obwohl er so „old school“ sei, brauche man die Sichtbarkeit des politischen Protestes [„visibility of political protest“] auf der Straße. Natürlich gäbe es andere Wege, Politik schneller zu ändern, dafür bräuchte es aber starke, kühne [„bold“] und risikofreudige politische Anführer – Jesusgestalten [„a Jesus figure“], die sich aber nicht abzeichnen würden [„but where are they?“].[13]

Aus der im eingespielten Diskussionsausschnitt problematisierten Wandlung der Widerstandskultur im privaten und öffentlichen Raum solle laut Florian Wobser und Tom Gehrke nun ein historisch-systematischer Rückblick zum „Sinn des Privaten“ erfolgen, um damit verbundene Problemhorizonte aufzuzeigen.

Teil 2 – Vom einstigen Sinn des Öffentlichen

2.1 Immanuel Kant

Erster wichtiger Philosoph in diesem Zusammenhang sei Immanuel Kant, dessen Aufklärungsphilosophie durch die Konzepte der Freiheit durch Autonomie, Publizität und Moralität bedingt sei (Folie 10). Realisiere ein autonomer Mensch den Vernunftgebrauch, so sei dieser nach Kant in einen privaten und öffentlichen Gebrauch zu unterteilen. In dieser Unterteilung seien jedoch die Kategorien „privat“ und „öffentlich“ genau entgegengesetzt zum modernen Gebrauch definiert (Folie 11):

11 Anm. d. Pr.: Bieber erklärte vorangehend neben der Relevanz moderner sozialer Netzwerke [„social networks“] zum Zweck des Ausdrucks öffentlicher Unzufriedenheit [„public anger“] die Bedeutung klassischer Ausdrucksformen des Protestes auf der Straße [„the street“] als mächtigste Verbindung [„most powerful link“] zwischen politisierter Öffentlichkeit [„politicized public“] und politischem System [„political system“], sodass Protestbewegungen [„the movement“] zwar auf das Potential sozialer Netzwerke [„power of the social networks“] und digitaler Kommunikation [„digital communication“] setzen könnten, zugleich aber auch Wege auf „die Straße“ finden müssten [„has to find ways to get out on the street“] - der Mangel an Anknüpfung an traditionelle Protestformen [„they lack the connection“] sei somit zentrales Problem im modernen Netzaktivismus.

12 Anm. d. Pr.: Eine freie Software zur Anonymisierung des eigenen Internetverkehrs und der Umgehung von Internet-Zensur: https://www.torproject.org/ (zuletzt aufgerufen: 02. Okt. 2015).

13 Konferenz „Einbruch der Dunkelheit“ vom 25.-26. Jan 2014 in Berlin; der im Vortrag eingespielte Ausschnitt bezieht sich auf den Zeitindex 00:37:30-00:42:30 beginnend mit der Antwort von Appelbaum auf Bieber im Beitrag „Transparenz: Was können wir von Manning, Assange und Snowden lernen?“ vom 26. Jan 2014, online abrufbar unter: http://www.dctp.tv/filme/edd-transparenz/ (zuletzt aufgerufen: 02. Okt. 2015).

„[...] der öffentliche Gebrauch seiner Vernunft muß jederzeit frei sein, und der allein kann Aufklärung unter Menschen zustande bringen; der Privatgebrauch derselben aber darf öfters sehr enge eingeschränkt sein, ohne doch darum den Fortschritt der Aufklärung sonderlich zu hindern. Ich verstehe aber unter dem öffentlichen Gebrauche seiner eigenen Vernunft denjenigen, den jemand als Gelehrter von ihr vor dem ganzen Publikum der Leserwelt macht. Den Privatgebrauch nenne ich denjenigen, den er in einem gewissen ihm anvertrauten bürgerlichen Posten oder Amte von seiner Vernunft machen darf.“[14]

Unabhängig von der Frage nach diesen Definitionen ergebe sich aber die Frage, warum Kant diese Trennung vornehme und inwiefern sie sinnvoll sei. Zur Klärung dieser Frage solle die Position von Jürgen Habermas herangezogen werden.

2.2 Jürgen Habermas

Als Theoretiker des 20. Jahrhunderts sähen Florian Wobser und Tom Gehrke Jürgen Habermas in der Tradition Kants (Folie 12). Vertreten werde die These, dass Habermas vor seiner späteren Idee der Emanzipation durch kommunikatives Handeln früh bereits die Tradition des Begriffes der Publizität von Kant aufgreife. Diesbezüglich stelle sich zwar das Problem der philosophischen Entwicklung von Habermas. Im Vergleich der 1960er und 1980er sei bei ihm das aus der Auseinandersetzung mit der frühen Frankfurter Schule mitgetragene Konfliktfeld zwischen System und Lebenswelt in den Hintergrund getreten. Nun liege zunehmend ein diskursethisches, konsensorientiertes Verfahren im Zentrum seiner Philosophie. Seine Form von deliberativer Demokratie stelle aber noch immer einen Bezug zu Kant her, zeige zugleich jedoch „blinde Flecken“ in Bezug auf Phänomene wie „Macht“. Beispielsweise werde der Bereich, welcher bei Kant unter den Begriff des Privaten fällt (also etwa Vernunfteinschränkungen aufgrund von Amtswürden), in der Diskursethik von Habermas nicht kritisch genug reflektiert. Am Beispiel des frühen Werkes „Strukturwandel der Öffentlichkeit“ von 1962 lasse sich nachweisen, dass der jüngere Habermas den Antagonismus von „kritischer Publizität“ und „bloß veranstalteter Publizität“ in Bezug auf die „politisch fungierende Öffentlichkeit“ noch stärker im Blick hatte als in seinem weniger antagonistischen, transzendental-diskursiven späten Denken (Folie 13):

„[...] Voraussetzungen einer politisch fungierenden Öffentlichkeit: die objektiv mögliche Minimalisierung der bürokratischen Dezisionen und eine Relativierung der strukturellen Interessenkonflikte nach Maßgabe eines erkennbaren Allgemeininteresses – diesen Voraussetzungen läßt sich heute nicht mehr schlechthin ein utopischer Charakter vindizieren. Die Dimension der Demokratisierung sozialstaatlich verfaßter Industriegesellschaften ist nicht von vornherein limitiert durch eine […] erwiesene Undurchdringlichkeit und Unauflösbarkeit der irrationalen Beziehungen sozialer Macht und politischer Herrschaft. Der Streit einer kritischen Publizität mit der zu manipulativen Zwecken bloß veranstalteten ist offen.“[15]

14 KANT, I.: „Beantwortung der Frage: Was ist Aufklärung?“, in: „Was ist Aufklärung?“, Reclams Universal-Bibliothek Nr. 9714, 2006, 11.

15 HABERMAS. J.: „Strukturwandel und Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft.“, Darmstadt; Neuwied, [15]1984.

Sowohl bei Kant als auch beim späteren Habermas würden sich also Einseitigkeiten zeigen, die mittels der sozialphilosophischen Kritik des 19. und 20. Jh. verdeutlicht werden könnten. Verzichtet werde dabei auf die Beiträge der frühen Frankfurter Schule wie derer Walter Benjamins und Theodor Adornos. Gegen Letzteren richte sich das erwähnte Zitat von Habermas (Folie 13), konkret gegen den von Theodor Adornos und Max Horkheimer geprägten Begriff des unumgänglichen und undurchdringlichen Verblendungszusammenhangs. Desweiteren erfolge keine Besprechung einer konservativen Institutionentheorie von Philosophen wie Arnold Gehlen und ihrer Überlegungen zum Mängelwesen Mensch.

Es folgte eine Beschäftigung mit den Kritikern des klassischen Aufklärungs- und Öffentlichkeitsbegriffes (Folie 15).

Teil 3 – Vom Unsinn des Nicht-Öffentlichen

Im Spannungsfeld von Liberalismus und Kommunitarismus einerseits sowie von Moral und Ethik andererseits würde sich eine Auseinandersetzung mit dem frühen Wilhelm von Humboldt etwa zum Spannungsfeld zwischen Staat und Individuum anbieten. Aus Zeitgründen beziehe sich dieser Teil jedoch lediglich auf Georg Wilhelm Friedrich Hegel.

3.1 Georg Wilhelm Friedrich Hegel

Hegels Philosophie unternehme ein dialektisches Überschreiten der Trennung des öffentlichen und privaten Vernunftgebrauches bei Kant (Folie 16). Der Nachteil dieses Ansatzes bestehe in der Einseitigkeit der Betrachtung des (preußischen) Staates als gesetzgebende Gewalt und Garant der Sittlichkeit. Es wurde dabei folgender Frageimpuls eingeworfen: Könne man aus der Perspektive von Hegel mit Blick auf die Gegenwart staatliche Institutionen wie NSA und GCHQ, deren Gebäudekomplexe bereits in architektonischer Hinsicht überdeutlich Hermetik und Unangreifbarkeit ausdrücken würden, als staatliche Garanten der Sittlichkeit bezeichnen (Folie 17)? Und wie wäre dieser Zusammenhang zu beurteilen?

Nach diesem kurzen Umriss zum Thema Staatlichkeit und Sittlichkeit erfolge nun ein Exkurs zu Staat, Ökonomie und Recht bei Karl Marx und Friedrich Engels sowie deren Kritik an Kant und Hegel.

3.2 Karl Marx und Friedrich Engels

Die Ausführungen dieses Abschnittes bezögen sich auf die Kritik von Marx an der bürgerlichen und politischen Ökonomie (Folie 18). Die bürgerliche Ökonomie nach Marx beute Arbeiter_innen zugunsten des Profits durch Entfremdung von ihren Produktionsmitteln aus, wodurch Arbeiter_innen vollständig in den bürgerlichen Dienst des Kapitals gestellt würden. In diesem Zusammenhang solle das Zitat des Facebook-Gründers Mark Elliot Zuckerberg als einem Vertreter der bürgerlichen Ökonomie stehen und in Gegenüberstellung zum Kommunistischen Manifest die möglichen Folgen der Analyse von Marx und Engels verdeutlichen (Folie 19). Zuckerberg: „Privacy is no longer a social norm.“[16] Marx/Engels: „Das

16 JOHNSON, B: „Privacy no longer a social norm, says Facebook founder“, theguardian, com, 11. Jan 2010, online abrufbar unter: http://www.theguardian.com/technology/2010/jan/11/facebook-privacy – Kurzlink: http://kurzlink.de/m5DHzCtwd (zuletzt aufgerufen: 02. Okt. 2015).

Bedürfnis nach einem stets ausgedehnteren Absatz für ihre Produkte jagt die Bourgeoisie über die ganze Erdkugel. Überall muß sie sich einnisten, überall anbauen, überall Verbindungen herstellen.“[17]

Die entfesselte Ökonomie im Dienst des Kapitals erweise im Zusammenhang mit der Aussage „privacy is no longer a social norm“ folgenden Zusammenhang: Bürgerliche Ökonomen erhielten die Möglichkeit, soziale Normen neu zu definieren und könnten dabei auf die Unterstützung von ökonomisch abhängigen Nationalstaaten bauen. Zu diskutieren sei die Frage, ob soziale Netzwerke wie etwa Facebook sich heute zugunsten des Profits in die privaten Verhältnisse der Menschen einnisteten. Während Hegel das Private des Menschen dem Staat unterwerfe, sei diese Unterwerfung bei Marx und Engels durch den Mehrwert bedingt. Beide Positionen greifen Kants Trennung zwischen „Privatem“ und „Öffentlichem“ an und seien auch antagonistischer als etwa die Position von Habermas.

Es folgte ein Ausschnitt der „re:publica“, einer jährlichen Berliner Konferenz, die sich Phänomenen der digitalen Gesellschaft widmet, vom Mai 2014. Die US-amerikanischen Journalistinnen Sarah Harrison, auch bekannt in ihrer Funktion als Wikileaks-Aktivistin, sowie Alexa O'Brien, bekannt durch Ihre Berichterstattung zum Prozess von Chelsea Manning, kamen wie folgt zu Wort:

3.3 Exkurs: „re:publica'14“ - „From USA to USB“ (S. Harrison, A. O'Brien)

Ein Publikumsgast fragte Harrison, wie die Welt, in welcher Harrison leben wolle, Harrisons Meinung nach beschaffen sein solle: Ob dies eine Welt frei verfügbarer Informationen sei [„like free information for everyone“] oder eine Welt, in der Privatsphäre respektiert werde [„where privacy is respected“] sowie die Frage, inwiefern dies aufgrund der Masse an gesammelten Daten [„the amount of technical data around us exploding“] überhaupt noch möglich sei. Harrison bekräftigte die Problematik der über die Menschen bereits gesammelten Daten [„there is a problem with […] the amount of data that has been collected […] so far“] und den Willen der Geheimdienste, diesen bereits riesigen Datenbestand immer weiter auszubauen [„let's get it all“]. Zudem betonte sie den harten Kampf, diesem Verhalten und der dahinterliegenden Psyche der Geheimdienste entgegenzuwirken [„to backtrack from that […] to get the psyche of these people to actually change is a very tough […] battle“]. Sie glaube an die Notwendigkeit von Privatsphäre von Normalbürgern [„I believe in the privacy of individuals like us“], aber daneben müsse vollständige Transparenz [„there should be complete transparency“] über jene Mächtigen [„powerful people“] möglich sein, die über das Potential verfügten, über ihre Mitmenschen zu herrschen [„that have […] ability to dominate over us“]. Ebenso sei vollständige Offenlegung notwendig, wenn es um unsere Geschichte und die dazugehörigen historischen Archive gehe [„when it comes to our history and creating our historical archive being in the public records, that's another area of information which I think should be fully published“]. Das aktuelle Problem [„the problem we now have“] bestehe in einem unausgewogenem Gleichgewicht [„balance“] von Gesellschaften, deren Regierungen alles für sich behielten [„governments keeping everything private“] und zugleich alle Informationen über ihre Bürger sammelten [„they collecting all of our personal informaton“]. Für eine emanzipatorische Veränderung müsse dieses unausgewogene Gleichgewicht korrigiert werden [„rectifying this balance changing it“].

17 MARX, K.; ENGELS, F.: „Manifest der Kommunistischen Partei“ (1848), in: „Karl Marx - Philosophische und ökonomische Schriften“, Reclams Universal-Bibliothek Nr. 18554, 2008, 85.

Zusammen mit O'Brien diskutierte Harrison desweiteren das Problem der Auslagerung von Geheimdiensttätigkeiten mit Hilfe von privaten Unternehmen, zu deren Mitarbeitern auch Edward Snowden gehörte, welche nicht über die selbe Haftbarkeit oder Verantwortlichkeit wie Regierungen [„the corporations don't have the same […] liability that governments have“], jedoch über die selben Überwachungsmöglichkeiten verfügten. So sei die Frage nach Kontrolle der Geheimdienste [„trying to control it“] sehr komplex und nach Ansicht Harrisons nur durch deutliche Budgetkürzungen zu erreichen [„the only way to do it is to start thinks like a huge budget cut“], um die Möglichkeiten der Geheimdienste einzuschränken [„you really need to completely minimize the abilities of these agencies“]. Andernfalls würden sie nur weiter wachsen [„or it's impossible to stop – it will just keep growing“].[18]

Sich an den gezeigten Konferenzausschnitt anschließende Fragen zur offenkundig schwierigen trennscharfen Unterscheidung der von Harrison genannten Bereiche könnten an dieser Stelle von Tom Gehrke und Florian Wobser genauso wenig diskutiert werden wie umfassende systematische Fragen der philosophischen Bestimmung des Subjektes zwischen Moderne und Postmoderne mit Blick auf die folgenden Autoren. Diesbezüglich sei ein pragmatisches Verständnis schulübergreifender kritischer Theorie zugunsten praktischer Emanzipation nötig. Hinsichtlich des Privaten verschiebe sich die Perspektive von einer kritischen Gegenwartsdiagnose in Teil 1 über den emphatischen Begriff der Öffentlichkeit in Teil 2 (die jeweils dem Privaten in seinem differenzierten Verständnis gegenübergestellt wurde: das Private als Hort staatlicher Instanzen selbst bei Kant, daraufhin bei Hegel als dem Staat eigentlich unterworfen, zuletzt bei Marx und Engels als vor der Ökonomie und dem Staat zu schützen) hin zu einer radikalen Infragestellung des Binarismus aus Privatem und Öffentlichem selbst (speziell unter Rückgriff auf das sozialpolitische Phänomen der Macht) in Teil 3.

3.4 Michel Foucault

Im Folgenden gehe es um das Prinzip der Macht und den französischen Philosophen Michel Foucault. Wichtig zum Verständnis von Foucault sei sein Verständnis von Macht im Vergleich mit anderen Machttheoretikern, welches u. a. anhand seines Werkes „Der Wille zum Wissen. Sexualität und Wahrheit“[19] deutlich werde. Darin werde Macht anders als bei Karl Marx, Jean-Jacques Rousseau und Montesquieu als „komplexe strategische Situation in einer Gesellschaft“ definiert (Folie 22). Daher entfalle für Foucault die Trennung zwischen öffentlicher und privater Sphäre. Ein politisch regierbarer Machtraum durchdringe bei Foucault alle Bereiche des Lebens, so auch die intuitiv unterteilten Bereiche des Öffentlichen und Privaten. Das nach Kant potentiell mögliche autonome Subjekt könne für Foucault daher praktisch nicht existieren. „Aufklärung“ für das Subjekt bedeute im Sinne Foucaults die Selbstproblematisierung des Subjektes über seine eigene Historizität und Gegenwart. Kritik könne dabei nicht wie bei Kant auf den Erkenntnisprozess beschränkt sein, doch das Subjekt zeichne sich durch eine kritisch-politische Tätigkeit aus. Grundlegende Begriffe Foucaults zur Machttheorie fänden sich in

18 Konferenz „re:publica'14“ vom 05.-07. Mai 2014 in Berlin; der im Vortrag eingespielte Ausschnitt bezieht sich auf den Zeitindex 00:46:20-00:50:30 des Beitrages „WikiLeaks, Manning and Snowden: From USA to USB“ vom 06. Mai 2014, online abrufbar unter: https://www.youtube.com/watch?v=UPltW8wg6aI – Kurzlink: https://youtu.be/UPltW8wg6aI (zuletzt aufgerufen: 02. Okt. 2015).

19 FOUCAULT, M.: „Der Wille zum Wissen. Sexualität und Wahrheit Bd. 1.“, Frankfurt am Main, 1983.

dessen „Mikrophysik der Macht“[20], so das Kraftfeld der Macht, durch welche der Mensch erst zum Subjekt geformt, d. h. durch Macht bedingt und daher selbst subjektiviert werde. Aus der Perspektive Foucaults werde jeder Mensch in bestimmte Umstände der Gesellschaft hineingeboren und von diesen zum Subjekt geformt. Daraus entstehe ein sog. Kraftfeld der Subjektivierung, welches von der Geburt bis zum Tod wirke. Es stehe diesem Kraftfeld der Begriff der Selbsttechnologien gegenüber (Folie 23), welche sich aus christlichen Bußpraktiken entwickelten und im engen Zusammenhang mit der Pastoralmacht stehe. Die Selbsttechnologien stellten eine Form der Selbstthematisierung dar und als solche einen Rest der klassischen Autonomie. Impliziert werde durch sie eine verinnerlichte Verpflichtung zum erzwungenen Schuldbekenntnis, durch welche in einem inneren Dialog ein stetiger Abgleich des eigenen Verhaltens zur Norm stattfinde. Die Pastoralmacht vor der Zeit der Aufklärung stelle jene Macht dar, über die nur der Pastor verfüge, da er durch die Praxis der Beichte alles über den Beichtenden wüsste. Allein durch dieses Allwissen wirke die Pastoralmacht nach Foucault.[21] Eine solche Praxis münde in Sicherheitsdispositive. In Verbindung mit dem stetigen inneren Monolog der Selbsttechnologien und der dadurch ausgeprägten persönlichen Kategorien von „gut“ und „schlecht“ entstehe auch erst die Möglichkeit der Delinquenz, welche mit der Aufklärung paradoxerweise zugleich lückenloser Verfolgung ausgesetzt worden sei, da aufgrund der Industrialisierung der Schutz des steigenden Privatbesitzes hohe Priorität gewonnen habe, wodurch wiederum die allgemeine Delinquenz angestiegen sei. So habe sich das Prinzip einer lückenlosen Disziplinargesellschaft lange vor den Zeiten der Überwachung im Internet entwickelt. Daneben stehe der Begriff der Biopolitik Foucaults als eine Form des politischen Zugriffs auf den Körper der Menschen hinsichtlich der Regulierung seiner Fortpflanzung und Sexualität. Der Begriff der Gouvernementalität beschreibe das Konglomerat sämtlicher administrativer auf das Subjekt einwirkender institutionalisierter Machttechniken. Durch seine historische Diskursanalyse habe Foucault für die Zeit um 1800 einen gesellschaftlichen Transformationsprozess festgestellt, der sich durch das Prinzip der Disziplinargesellschaft kennzeichne. Diese funktioniere nach einem panoptischen Prinzip gemäß der Definition des englischen Philosophen Jeremy Bentham. Dieses habe vor allem als architektonisches Grundprinzip von Gefängnisbauten eine physische Umsetzung erfahren. Die architektonische Umsetzung dieses Prinzips ermögliche einem Einzelnen die Beobachtung sehr vieler zu überwachender Personen, durch verblendete Scheiben sogar ohne deren Wissen (Folie 24).

Eine solche Architektur erzeuge ein beständiges Gefühl, die eigene Person könne zu jedem Zeitpunkt beobachtet werden, sodass das eigene Verhalten entsprechend angepasst werde, da der Insasse gezwungen sei, von einer zeitlich lückenlosen Beobachtung ausgehen zu müssen. Dieses panoptische Prinzip wirke nach Foucault in allen staatlichen Institutionen vom Kindergarten bis zur Fabrik, welches eine Person äußerlich wie innerlich in einem panoptischen Raum situiere und sie damit unterwerfe bzw. subjektiviere. Im Zusammenhang mit dem bereits erwähnten (Sicherheits-)Dispositiv (in welche jedes

20 FOUCAULT, M.: „Mikrophysik der Macht : über Strafjustiz, Psychiatrie u. Medizin“, Berlin, 1976, Katalog der Deutschen Nationalbibliothek: http://d-nb.info/760381453 (zuletzt aufgerufen: 02. Okt. 2015).

21 Vgl. BUBLITZ, H.: „Im Beichtstuhl der Medien : die Produktion des Selbst im öffentlichen Bekenntnis“, Bielefeld, 2010, Katalog der Deutschen Nationalbibliothek: http://d-nb.info/998765023 (zuletzt aufgerufen: 02. Okt. 2015).

Individuum hineingeboren werde und daher auf die es umgebenden gesellschaftlichen Lebensumstände nur bedingt Einfluss habe) ergebe sich folgendes Bild: Das panoptische Prinzip wirke strukturell in der Biopolitik fort, mittels derer Zugriff auf Körper und Geist genommen würde und so in jedes Individuum eingepflanzt werde. Damit erwirke es eine flächendeckende Struktur des vorauseilenden Gehorsams, die sich ohne gedankliche Reflexion der betroffenen Individuen entfalte oder selbst über deren Reflexion erhaben sei.

3.5 Gilles Deleuze und Félix Guattari

Nach der Darstellung Foucaults in seinen Grundzügen folgte zum Abschluss des dritten Teils des Vortrages die Position zweier weiterer philosophischer Vertreter Frankreichs, vorgestellt von Florian Wobser: Gilles Deleuze und Félix Guattari (Folie 25). In Kontinuität zu Foucault hätten Deleuze und Guattari in den 1970er und '80er Jahren den Begriff der Kriegsmaschine geprägt, der in institutioneller, d. h. anti-institutioneller Hinsicht dem Begriff der Selbsttechnologie Foucaults entspreche und sich etwa gegen Ökonomie und Staatlichkeit richte. Dem entgegen stehe eine Diskontinuität bei Deleuze und Guattari gegenüber Foucault durch Verwendung des Begriffes der Meute. Einerseits überführen Deleuze und Guattari Foucaults „Mikrophysik der Macht“ in mikropolitische Prozesse. Im Vergleich zu Marx und Engels werde andererseits die Verwendung des klassischen Begriffes der Masse aufgegeben und durch punktuell und plötzlich auftretende Meuten ersetzt und radikalisiert. Die Mikropolitik der Meuten entspreche der Strategie der Kriegsmaschine, deren Re- und Deterritorialisierung als ein Werden innerhalb der Immanenz der Macht zu begreifen seien. Dadurch lasse sich auch in diesem Zusammenhang ein bestimmtes philosophisches Raumkonzept erkennen. Dieses sei bei Foucault jedoch vor allem ein technisch, institutioneller, architektonischer Raum. Bei Deleuze und Guattari jedoch werde ein Raum der Virtualität beschrieben, der mit einer Virtualisierung des panoptischen Prinzips einhergehe. Darüber hinaus falle bei Deleuze und Guattari verschärfend der Begriff der Kontrollgesellschaft. Das Prinzip des vorauseilenden Gehorsams werde in theoretischer Hinsicht als eine Verlagerung des Panopticons in die Psyche und Physis der Menschen verstanden. Institutionelle und biopolitische Prozesse fielen so verschärft zusammen. Diese Konzepte und Affekte der Menschen bzw. der Meuten stünden dadurch immer unausweichlich in Relation zur Aktualisierung ihrer Fremd- und Selbstkontrolle. Eine maximale Kolonialisierung des Privaten durch das etwa Staatliche oder ökonomisch Öffentliche – als Radikalisierung des frühen, aber nicht des späten Habermas – sei die unausweichliche Folge. Der Begriff der Mikropolitik sei ein vielfach diskutierter, bei dem es trotz unterschiedlicher Entwürfe immer um den Widerstand in Gegenüberstellung von Minoritäten zu Majoritäten gehe.

In zusammenfassender Betrachtung des Übergangs von Foucault zu Deleuze und Guattari meinten letztere über ersteren, Foucault gehöre zu den ersten Denkern, die eine allgemeine Wandlung der Disziplinargesellschaft hin zu einer Kontrollgesellschaft festgestellt hätten (Folie 26). Diese funktioniere nicht mehr durch Internierung, sondern durch unablässige Kontrolle und unmittelbare Kommunikation. Beide Gesellschaftsformen ließen sich mit bestimmten Maschinentypen in Beziehung setzen. Energetische Maschinen entsprächen den Disziplinargesellschaften, Computersysteme den

Kontrollgesellschaften, wie Deleuze 1990 feststellte.[22] Diese Diagnose der 1970er und 1980er Jahre wirke mit Blick auf die Gegenwart visionär und sei, etwa hinsichtlich ihrer Tendenz zur Überzogenheit, abwägend zu diskutieren.

Eine besondere Rolle spiele in diesem Zusammenhang der Begriff der Auto-Surveillance [„Selbst-Überwachung“], welcher in einem Gespräch zwischen Ron Deibert, einem kanadischen Medientheoretiker sowie Philip Banse, einem deutschen Journalisten der dctp GmbH, auf der re:publica 2014 thematisiert wurde. Grundlegend werde auch an diesem Interview, welches wie die zuvor eingespielten ebenfalls auf Berliner Boden abgehalten wurde, ersichtlich, dass die Stadt Berlin eine bedeutende Rolle für den bestehenden Diskurs zur Überwachungsaffäre spiele (Folie 27).

3.6 Exkurs: „re:publica'14“ - „Die dunkle Seite der Snowden-Leaks“ (R. Deibert, P. Banse)

Ron Deibert erklärte im eingespielten Interviewausschnitt, die Bevölkerung sei von der Überwachung wenig überrascht gewesen [„not that surprised about surveillance“], da es bereits ein etabliertes Konzept sei Informationen über die eigene Person herauszugeben [„used to giving away information already through concept“], zum Beispiel in Form von personenbezogenen Statusmeldungen in sozialen Netzwerken, bspw. Facebook, in welchem jedes Detail des eigenen Lebens veröffentlicht werde [„this is my place of work, here is my dog, this is my friend“].[23] Daraus habe sich eine Gesellschaft der Selbst-Überwachung [„auto-surveillance society“] entwickelt. Diese entstand daher nicht aus dem Nichts heraus [„out of nowhere“] und die Bevölkerung habe sich an diesen Zustand gewöhnt [„people were accustomed to“], auch durch Literatur und Fernsehen [„through fiction, through television“]. Erforderlich sei ein Nachweis für den Missbrauch [„evidence of abuse“] der von den Geheimdiensten gesammelten Daten durch die Regierung analog zur Watergate-Affäre [„along the lines of a Watergate scandal“] – dies würde Reformen auslösen [„that might trigger reforms“].

Deibert sprach zudem den meisten Regierungen der Welt [„most of the governments in the world“] die demokratischen Voraussetzungen ab, entsprechende Reformen anzugehen [„not democratic to begin with“]. Die derzeitige Entwicklung vieler Gesellschaften sei eine rückläufige in autoritäre Regierungssysteme [„sliding back into authoritarianism“]. Länder wie Thailand, Indonesien und Indien, immens wachsend durch Informationstechnologie [„massive growth in internet technologies“], würden die Technologien gestalten [„shaping the technologies“], welche die westliche Welt bald einsetzen werde [„that we use here very soon“], wobei es in diesen Ländern noch schwieriger sei, über die angemessene Verwendung derselben zu sprechen [„even more difficult to talk about proper capability“].

Banse problematisierte daraufhin Deiberts Aussage zu Watergate durch den Vergleich mit der bestehenden These, es bräuchte ein „Tschernobyl“, um den derzeitigen Kurs zu ändern [„a Chernobyl to

22 DELEUZE, G.: „Postskriptum über die Kontrollgesellschaften.“, in: „Unterhandlungen. 1972-1990.“, Frankfurt am Main, 1993, 254-262.

23 Anm. d. Pr.: Philip Banse fasste zuvor den bisherigen Dialog mit Deibert wie folgt zusammen: Hinsichtlich des aus einem kontrollierten Gleichgewicht geratenen Machtgefüges zwischen Staaten und Geheimdiensten müsse die Bevölkerung ein Machtgleichgewicht erst wieder aufbauen [„we have to re-establish […] the balance of power“], um Geheimdienste als Apparate einer Regierung wieder unter eine Kontrolle derselben zu bringen [„to […] really control those powers within the government“]. Das Bewusstsein für ein solches Prinzip [Anm. d. Pr.: der Notwendigkeit der Kontrolle von Geheimdiensten] sei verloren gegangen [„we […] lost track on […] those principles“]. Die nun folgende Frage an Deibert lautete, ob die Entrüstung [„the outcry“] der Bevölkerung groß genug sei, um das beschriebene Machtgleichgewicht wiederherstellen zu können [„to get this back“]. Der im Vortrag eingespielte Abschnitt setzt in der nun folgenden Antwort Deiberts ein, der die Frage zunächst verneint [„not right now“] und dies mit dem Zustand einer etablierten Selbst-Überwachung erklärt.

[…] turn the ship around“]. Banses Ansicht nach gäbe es bereits entsprechende Skandale [„we have those scandals“] in Form der Telefonüberwachung vieler Staatsoberhäupter [„the phones of […] thirty or fourty heads of state are being tabbed“], der Manipulation unzähliger Bestandteile der Internet-Infrastruktur [„manipulating countless of routers and hardware around the internet“], der Injektion von bösartigen Programmen in die Kommunikationswege hinein [„injecting code and malicious software into realtime internet conversation“] und entgegnete Deibert entsprechend mit der Frage, was denn noch Schlimmeres passieren könne [„what worse could happen“]. Deiberts Ansicht nach würden diese Beispiele die eindrucksvolle Macht der NSA demonstrieren [„demonstrates the awesome power of the NSA“]. Die Frage sei jedoch, ob sie die gesammelten Informationen missbrauchen [„abusing that information“]. Auf Nachfrage Banses hin, ob es für einen Missbrauch tatsächlich keine Anzeichen gäbe, entgegnete Deibert zwiegespalten, er habe diesbezüglich einerseits nichts außergewöhnlich Schlechtes vernommen [„I haven't seen something extraordinary bad“], andererseits sei deswegen aber auch nicht daraus zu schließen, dass ein Missbrauch nicht doch stattfinde [„that's not to say it might not be happening“]. Er sei der Meinung, dass es bis zur Aufdeckung schwerwiegender Konsequenzen der Überwachung [„major consequence that demonstrates the people why this is bad“] lediglich kleinere Reformen [„piecemeal reform“] gäbe. Banse wies darauf hin, dass Teile der Bevölkerung ihr Verhalten in Bezug auf politische Äußerungen [„Obama-talk on Facebook“] bspw. vor einer anstehenden Reise in die USA im Wissen einer allgemeinen Überwachung bereits ändern würden [„this kind of development is already going on“], um nicht Gefahr zu laufen mit unangenehmen Fragen am Flughafen [„questions at the airport“] konfrontiert zu werden. Deibert und Banse konstatierten einen bereits bestehenden Zustand der Selbstzensur [„self censoring“], woraufhin Banse fragte, ob dieser Umstand ausreichend sei, etwas zu ändern [„enough for people to really change“]. Deibert verneinte auch diese Frage mit der Erklärung, es sei die trickreiche Persönlichkeit der Überwachung [„that's the tricky character of surveillance“] sich langsam und geräuschlos in das Leben der Menschen zu schleichen [„it can creep slowly into ones life very silent“].[24]

Florian Wobser stellte im Nachklang zum eingespielten Interview die Problematik in den Raum, ob für gesellschaftlichen Wandel tatsächlich zunächst *konkreter* Missbrauch ähnlich der Watergate-Affäre nötig sei und warum der Umstand *allgemeiner* Überwachung nicht ausreiche.

3.7 Auf Spurensuche im öffentlichen Raum

Im Hinblick auf die Thematik „Vom Unsinn des Nicht-Öffentlichen“ lasse sich nun ein Bedeutungswandel feststellen. Die historische Emphase „das Private ist politisch“ (eine der emanzipatorischen Hauptthesen der politischen Reformbewegungen um und nach 1968) sei ein Beispiel für einen vergangenen Umgang mit dem „Unsinn des Nicht-Öffentlichen“, hinter der sich die These verberge, das Private müsse ein Öffentliches sein, um eine wirkliche Demokratie zu etablieren. Aktuell habe sich aber in überaus problematischer Weise die ehemals kritische Ausrichtung der Diagnose „Vom Unsinn des Nicht-

24 Konferenz „re:publica'14“ vom 05.-07. Mai 2014 in Berlin; der im Vortrag eingespielte Ausschnitt bezieht sich auf den Zeitindex 00:14:09-00:18:10 des Beitrages „Die dunkle Seite der Snowden-Leaks“, online abrufbar unter: http://youtu.be/vgmlkFQozxQ?list=PL2ROEjP_GuocZh77wFvm_4FwwgbvFFpuc – Kurzlink: http://kurzlink.de/BmaiHcW9u (zuletzt aufgerufen: 02. Okt. 2015).

Öffentlichen“ derart verschärft, dass die Annahme eines nicht-öffentlichen Bereiches ein Unsinn sei (und historisch in ihr kontrollgesellschaftliches Gegenteil umschlage).

Die Auseinandersetzung mit dem Theorem der Kontrollgesellschaft stehe im Zusammenhang mit der Frage nach weiteren Spuren, durch welche sich die Kontrollgesellschaft intuitiv nachweisen lasse bzw. in denen sie anschaulich werde. Eine solche Spurensuche müsse bspw. den „gläsernen“ Bürger sowie den „vermachteten“ bzw. kontrollierten Raum untersuchen. Zwei Beispiele würden die durch Foucault, Deleuze, Guattari u. a. kritisch reflektierten Phänomene der self-fulfilling prophecy (selbsterfüllende Prophezeiung) sowie des double-bind (Doppelbindungstheorie) verdeutlichen und Imperative, die notwendigerweise zu Verhaltensparadoxien führten, entlarven. Bspw. diejenigen, die in öffentlichen Wahlsprüchen nach den Anschlägen vom 11. Sep. 2001 den öffentlichen Raum dominierten. Fraglich sei, welche gesellschaftlichen Konsequenzen eine öffentliche Aufforderung wie „If you see something say something“ [„Wenn sie etwas sehen, melden sie es!“] zwischenmenschlich nach sich ziehe (Folie 29). Florian Wobser merkte an, dass ihm persönlich dieser öffentliche Imperativ nicht erstmalig in New York, sondern in Mumbai (Indien) aufgefallen sei, einer Stadt, die in den 2000er Jahren ebenfalls Tatort terroristischer Anschläge gewesen sei. Imperative wie diese würden noch befremdlicher auf das eigene Verhalten wirken, wenn sie in Kombination mit dort zusätzlich vorfindlichen Aufforderungen wie „be suspicious of anything unattended“ [„Sei misstrauisch gegenüber allem, was unbeaufsichtigt ist!“] stünden.

Das zweite Beispiel betreffe das „nothing to hide“-Argument [„nichts zu verbergen“-Argument), welches auf den hochrangigen Mitarbeiter des Unternehmens Google, Eric Emerson Schmidt, zurückgehe (Folie 30). Dieses besage, eine private Handlung von vorneherein zu unterlassen, wenn diese auf keinen Fall aus dem Privaten ins Öffentliche gelangen solle.[25] Eine solche Argumentation wirke sich in fragwürdiger Weise auf die Entwicklung einer Gesellschaft aus und müsse daher diskutiert werden.

Deleuze und Guattari beschrieben aufgrund ihrer psychoanalytischen Prägung die uns umgebende Welt, zu der speziell mit Blick auf die Spannungen zwischen dem Privaten und Öffentlichen die o. g. Imperative gehörten, als eine paranoid-schizoartige, was durch ein Zitat deutlich werde, welches den Kapitalismus bereits in den 1970er Jahren wie folgt beschreibe (Folie 31):

„Ein System wie der Kapitalismus leckt auf allen Seiten, es leckt, und dann dichtet der Kapitalismus die Risse ab, macht Knoten. Sorgt für Verklammerungen, um zu verhindern, daß die Fluchten zu zahlreich werden. [...] Doch bislang hat es auf dem revolutionären Feld keine Kriegsmaschine gegeben, die auf

25 Anm. des Pr.: Die vollständige Aussage Schmidts lautete: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time, and it's important, for example that we are all subject in the United States to the Patriot Act. It is possible that that information could be made available to the authorities." [„Wenn es Dinge gibt, von denen niemand erfahren soll, sollten sie diese Dinge von vorneherein unterlassen; aber wenn sie wirklich eine solche Privatsphäre benötigen ist die Wirklichkeit so, dass Suchmaschinen, Google eingeschlossen, solche Informationen für eine gewisse Zeit bewahren und es ist bspw. wichtig, dass wir alle in den Vereinigten Staaten dem [USA] PATRIOT Act unterliegen [Anm. d. Pr.: **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **Act -** Gesetz zur Einigung und Stärkung Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu blockieren]. Es ist möglich, dass diese Informationen den gesetzlichen Behörden verfügbar gemacht werden könnten.“] Quelle: NEWMAN, J.: „Google's Schmidt Roasted for Privacy Comments“, PCWorld, 11 Dez. 2009, online abrufbar unter: http://www.pcworld.com/article/184446/googles_schmidt_roasted_for_privacy_comments.html – Kurzlink: http://kurzlink.de/WxVhD1SSj (zuletzt aufgerufen: 02. Okt. 2015).

ihre Weise nicht auch etwas ganz anderes reproduziert hätte, nämlich einen Staatsapparat, den Organismus der Unterdrückung schlechthin.“[26]

Dieses Beispiel einer philosophischen Sichtweise der 1970er Jahre entspräche (aufgrund der Tendenz zur Übertreibung) nicht vollständig der Position Florian Wobsers und Tom Gehrkes, eine Reflexion dieser Gedanken wäre allerdings im Hinblick des Gesamtzusammenhangs der aktuellen globalen Überwachungsaffäre ein lohnenswertes Ziel, da zumindest die hier verwendete Metaphorik von „Lecks“ und „Fluchten“ in besonderer Weise mit den jüngsten politischen Ereignissen und politischen Strategien im Zusammenhang stünden (Folien 32-34) und die Übertreibung im gewählten Zitat hier den Sachverhalt veranschauliche.

Aufgrund der vorangeschrittenen Vortragszeit verzichteten Florian Wobser und Tom Gehrke auf theoretische Vertiefungen mittels des US-amerikanischen Literaturtheoretikers Michael Hardt und dem italienischen Politikwissenschaftler Antonio Negri anhand ihrer Werke „Empire“[27] und „Multitude“[28], durch welche die Überwachungsaffäre auch in einem globalisierungskritischen Zusammenhang untersucht werden könne. Ebenso müsse auf interessante Aspekte der Gegenwartsanalyse in den Werken des Berliner Professors Byung-Chul Han über die Begriffe „Transparenz“[29] und „Schwarm“[30] verzichtet werden.

Teil 4 als Abschluss des Gastvortrages beschäftige sich mit der Frage „Was tun?“ hinsichtlich der Möglichkeiten zum erörterten Befund der Überwachungsproblematik aus der Perspektive kritischer Theoretiker aus Frankfurt und Frankreich (Folie 36).

Teil 4 – Vom Un/Sinn des Öffentlichen/Privaten

Zu den Möglichkeiten der Positionierung gegen den Zustand der Überwachung zählte Florian Wobser informationelle Technologien wie Kryptographie als subversive praktische Strategien auf (Folie 37-38), die allerdings nicht nur zum Zweck einer Kompensation eingesetzt werden sollten. Daneben gehöre der Bereich Kunst fest in den Bereich der kritischen Theorie. welcher sich in diesem Zusammenhang nicht zuletzt auch nahe am Bereich des investigativen Journalismus bewegen könne (Folie 39). Beispielhaft dafür sei ein Vortrag im Rahmen der „transmediale 2014“, einem – erneut – Berliner Festival für Medienkunst und digitale Kultur (Folie 40).

4.1 Exkurs: „transmediale 2014“ - „Art as Evidence“ (T. Paglen)

Der US-amerikanische Künstler Trevor Paglen stellte unter der Überschrift „Art as Evidence“ [„Kunst als Beweismaterial“] Möglichkeiten dar, mittels Kunst die menschliche Wahrnehmung für die Individuen

26 DELEUZE, G.: „Fünf Thesen über die Psychoanalyse.“, in: Die einsame Insel. Texte und Gespräche von 1953-1974.“, Hg. D. Lapoujade, Frankfurt am Main, 2003, 398-407.

27 Hardt, M.; Negri, A.: „Empire : die neue Weltordnung. Aus dem Engl. von Thomas Atzert und Andreas Wirthensohn“; Frankfurt (Main)/New York, 2003, Katalog der Deutschen Nationalbibliothek: http://d-nb.info/96572364X (zuletzt aufgerufen: 02. Okt. 2015).

28 Hardt, M.; Negri, A.: „Multitude : Krieg und Demokratie im Empire. Aus dem Engl. übers. von Thomas Atzert und Andreas Wirthensohn“; Frankfurt (Main)/New York, 2004, Katalog der Deutschen Nationalbibliothek: http://d-nb.info/971011737 (zuletzt aufgerufen: 02. Okt. 2015).

29 Han, P.: „Transparenzgesellschaft“; Berlin, 2012, Katalog der Deutschen Nationalbibliothek: http://d-nb.info/1018043977 (zuletzt aufgerufen: 02. Okt. 2015).

30 Han, P.: „Im Schwarm : Ansichten des Digitale“; Berlin, 2013, Katalog der Deutschen Nationalbibliothek: http://d-nb.info/1028588631 (zuletzt aufgerufen: 02. Okt. 2015).

umgebende historische Momente zu erweitern [„what I want out of art is [...] developing ways of seeing […] things that help us see the historical moment that we are living in“]. Exemplarisch dafür seien kleine Partikel [„little bits“] einer gewissermaßen künstlerisch archivierten dunklen Materie z. B. verdeckter militärischer Operationen [„archival dark matter of covered operations“], die sich in Form von Uniform-Aufnähern [„uniform patches from military projects“] paradoxerweise verrieten. Der Umstand, dass das [US-]Militär tatsächlich Erkennungszeichen sogar für die Uniformen der Mitarbeiter *geheimer* Projekte [„black projects“] anfertige [Vgl. Abb. 1 u. 2], sei eine der skurrilsten Formen von Kunst, der man begegnen könne [„this is one of the most bizarre forms of art that you'll ever run across“].[31]

Derartige Kunststrategien seien nach Florian Wobser und Tom Gehrke eine Form der unbedingten Aufklärung und Bildung. Dies werde auch an Ausstellungen des chinesischen Künstlers Ai Weiwei deutlich, der in einer Kunstinstallation auf Alcatraz auch Bezug auf Edward Snowdens Grundsatz *„privacy is a function of liberty“* [„Privatsphäre ist ein Ergebnis/eine Folge der Freiheit“][32] nahm und damit ebenfalls Kunst als Medium zur Aufklärung praktiziere (Folie 41-42).

Abb. 1: aus dem Vortrag „Art as Evidence“. Trevor Paglen (Festival „transmediale 2014 afterglow“]. DE/Berlin 2014. Zeitindex: 00:13:03. Übersetzung: „Sonderprojekte – Testflugstaffel“.

Abb. 2: aus dem Vortrag „Art as Evidence“. Trevor Paglen (Festival „transmediale 2014 afterglow“]. DE/Berlin 2014. Zeitindex: 00:14:03. Übersetzung: „Sensorjäger – Kein Land (darf) zu eigenstaatlich (sein)“.

Daneben könne als weiteres emanzipatorisches Mittel etwa die Infrastruktur und der Rechtsschutz für Whistleblowing [„Skandalaufdeckung“] ausgebaut werden (Folie 43). Ebenso sei das Bildungssystem mehr denn je hinsichtlich der Ausbildung zeitgemäßer elementarer Kulturtechniken gefordert, bspw. in Bezug auf den problematischen Zustand des Informatikunterrichtes als Teil der Medienbildung. Die Verbesserung der angesprochenen Bereiche stünde indirekt zur Herausbildung politisch-juridischer Prozesse in Beziehung, die zugleich auch explizit zu fördern seien, da sie entgegen einer rein formalen Demokratie das Recht wirksamer an aktuelle politische Systeme anpassen könnten (Folie 44).

Der Abschlussgedanke des Vortrages bezog sich auf die Möglichkeit, den im Vortrag entwickelten theoretischen Rahmen mit praktischen Handlungsoptionen zu verbinden. Umsetzbar sei dies nicht zuletzt durch die Idee des „gemeinsamen Dekonstruierens“ von „sozio-politisch relevanten binären

31 Festival „transmediale 2014 afterglow“ vom 29. Jan - 02. Feb. 2014 in Berlin; der im Gastvortrag eingespielte Ausschnitt bezog sich auf Zeitindex 00:00:00-00:01:00 sowie 00:12:00-00:14:00 des Beitrages „Art as Evidence“, online abrufbar unter: https://www.youtube.com/watch?v=SDxue3jGAug – Kurzlink: https://youtu.be/Sdxue3jGAug (zuletzt aufgerufen: 02. Okt. 2015).

32 Anm. d. Pr.: Das vollständige Zitat Snowdens lautet: *"Most reasonable people would grant that privacy is a function of liberty. And if we get rid of privacy, we're making ourselves less free."* [„Vernünftigen Menschen würden einräumen, dass Privatsphäre eine Folge der Freiheit sei. Und wenn wir Privatsphäre beseitigen berauben wir uns selbst der Freiheit“] Quelle: RUSBRIDGER, A.; MACASKILL, E.: „Edward Snowden interview - the edited transcript“, theguardian.com, 18. Jul. 2014, online abrufbar unter: http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript - Kurzlink: http://kurzlink.de/9dr1tO21E (zuletzt aufgerufen: 02. Okt. 2015).

Kategorien“ (Folie 45). Dieser Gedanke beziehe sich auf ein philosophisches Verfahren Jacques Derridas (einem Zeitgenossen von Foucault, Deleuze und Guattari): die Strategie der différance.

4.2 Jacques Derrida

In der Anwendung von Derridas Strategie der différance gehe es in Bezug auf den Kontext der Auseinandersetzung mit dem Privaten darum, immer fortlaufend die Beziehungen zwischen Unsinn und Sinn des Öffentlichen wie auch des Privaten neu zu relationieren und so durch geltende Systeme verdrängte Zusammenhänge auch diskursiv zu äußern (Folie 46). Auf diesem Wege könne eine auch emanzipatorische Performativität mit juristischer Relevanz bewirkt werden (Folie 47). Darin bestehe zugleich der von Florian Wobser und Tom Gehrke vermutete Sinn der Veranstaltung „Vom Sinn des Privaten“ im Rahmen der stud. Initiative „Jahr 1 nach Snowden“ und damit auch ihr eigenes Sprechen als Ausdruck des Sinns des Privaten: Dekonstruieren erlaube nämlich nicht, einen der vier Pole in der Gegenüberstellung von Unsinn, Sinn, öffentlich und privat auf Kosten eines anderen zu verabsolutieren.
Derrida sei Vordenker vieler Phänomene, die im Vortrag zur Sprache kamen, bspw. die des massenmedialen Archivs, verschiedener Formen der Öffentlichkeit, der unbedingten Gastfreundschaft (die sich heute auf die Problemfelder um das Asylrecht anwenden ließen) und ebenso der Etablierung einer unbedingten Universität.
Ein Zitat Derridas aus dem Jahr 1993, welches die Strategie der Dekonstruktion sowie die besondere Relevanz der Gerechtigkeit neben jener der Freiheit verdeutliche, solle an Michaela Zinke und ihre im engeren Sinne juristische Perspektive mit den folgenden Worten überleiten:
„Doch das Paradoxon, das ich in die Diskussion einbringen möchte, hat folgende Gestalt: Weil sie sich dekonstruieren läßt, sichert die Struktur des Rechts oder – wenn Sie wollen – der Gerechtigkeit, der Justiz als Recht, die Möglichkeit der Dekonstruktion. Wenn es etwas gibt wie die Gerechtigkeit als solche, eine Gerechtigkeit außerhalb oder jenseits des Rechts, so läßt sie sich nicht dekonstruieren. Ebensowenig wie die Dekonstruktion selbst, wenn es so etwas gibt. Die Dekonstruktion ist die Gerechtigkeit.“[33] (Folie 48)

Gastvortrag von Michaela Zinke

Der Fokus von Michaela Zinke liege auf der Frage, wie sich das Verbraucher_innenverhalten hinsichtlich der Privatsphäre verhalte und ob es sich durch die Enthüllungen von Edward Snowden gewandelt habe. Es sei ein Versuch, aus der Praxis des Verbraucherschutzes zu berichten.

1. Privatsphäre aus Sicht der Verbraucher

Privatsphäre sei in der Regel ein grundsätzlicher Wunsch der Verbraucher_innen. In aktuelle Umfragen hätten 37% der Befragten ihre Besorgnis um ihre Privatsphäre in der Nutzung des Internets zum Ausdruck gebracht. 66% der Internet-Verweigerer_innen lehnten eine Benutzung des Internets aus ähnlichen Gründen der Gefährdung des Datenschutzes ab. Als zukünftige gesellschaftliche Risiken

33 DERRIDA, J.: „Gesetzeskraft. Der »mystische Grund der Autorität«.“, Frankfurt am Main, 1991.

empfänden 65% der Verbraucher_innen den Missbrauch ihrer persönlichen Daten. Diese Beispiele seien exemplarisch für Umfragen zur Privatsphäre dieser Art.

Zugleich sei jedoch festzustellen, dass sich Verbraucher_innen nicht entsprechend ihrer Bedenken zum Schutz ihrer Privatsphäre verhielten und die Preisgabe persönlicher Daten die Regel sei. Beobachtungen des Verbraucherschutzes der letzten Jahre habe dieser Widerspruch zwei Gründe. Der erste bestehe in der völligen Intransparenz des digitalen Marktes, der zweite in der mangelnden Spürbarkeit von Überwachung.

2. Intransparenz im digitalen Markt

Festzustellen sei, dass der digitale Markt die Nutzer_innen in Waren umwandle. Private Daten seien folglich in diesem Zusammenhang zum Zahlungsmittel geworden. Vorlieben, Ansichten und Einschätzungen würden digital gesammelt und ausgewertet. Problematisch sei daran vor allem, dass zum einen keine Institution mit entsprechenden Kapazitäten und Kompetenzen den Umgang mit dieser neuen Form von Währung überwache und zum anderen eine angemessene Eigenkontrolle nicht feststellbar sei.

Der status quo eines von Monopolen kontrollierten Marktes (bspw. durch Google, Facebook, Amazon und Apple) biete Verbraucher_innen kaum Möglichkeiten, Alternativen für etablierte Dienstleistung zu nutzen. Zudem erschwere der Netzwerkeffekt, durch welchen Verbraucher_innen nur jene Dienste wählten, die auch das eigene soziale Umfeld nutze, einen Wechsel zu alternativen Diensten.

Die umfangreiche Sammlung an Daten großer Unternehmen über ihre Nutzer_innen umfasse bspw. Name, Wohnort, Kreditkartendaten, Bewegungsprofile und Einkaufsverhalten, einschließlich der Daten des jeweiligen sozialen Umfeldes.

Der Mechanismus digitaler Überwachung werde deutlich, vergleiche man den Vorgang eines Einkaufsgeschäftes in realen und der virtuellen Welt. Der Kaufvorgang bei einem klassischen Bäcker offenbare dem Verkäufer nicht Informationen wie Name, Alter, Wohnort, den individuellen Anfahrtsweg zum Bäcker sowie Gewicht und sportliche Tätigkeiten der Kund_innen. Ein Geschäft des digitalen Marktes jedoch greife diese Daten in der Regel in großem Stil ab. Dies finde einerseits mit Unwissenheit der Kund_innen statt, andererseits aber auch mit kaum kalkulierter Duldung seitens der Kund_innen.

Verbraucher_innen hätten kaum Informationen über Zahl und Umfang der über sie erstellten Nutzerprofile, da die dahinterliegenden Algorithmen geheim seien. Anhand solcher Algorithmen werde jedoch häufig über den Umgang mit Nutzer_innen bestimmt, beispielweise in Bezug auf personalisierte Werbung. Dieses etablierte Verfahren werde es zukünftig ermöglichen, Produktpreise auf Nutzer_innen hin zuzuschneiden, Versicherungstarife zu personalisieren, über die Vergabe von Studienplätzen auf neue Weise zu entscheiden und Verbrechen zuzuschreiben, bevor sie begangen würden.

Das allgemeine Informationsungleichgewicht zwischen Verbraucher_innen und Unternehmen verstärke den Effekt, Überwachung nicht wahrzunehmen vor allem auch dadurch, dass seitens der Unternehmen nur solche Informationen über das Sammeln von Kundendaten bereitgestellt würden, die schwer wahrnehmbar seien. Deutlich werde dies daran, dass bspw. der Ausdruck der Allgemeinen Geschäftsbedingungen einer Software wie iTunes 45 DIN A4-Seiten umfasse und damit aus

Verbraucher_innenperspektive vollumfänglich nicht erfassbar sei. Schon auf sprachlicher Ebene werde dies deutlich, da sich mit den im Beispiel erwähnten AGB dem Zweck nach eine juristische Absicherung mit entsprechender Komplexität stattfinde, die nicht dazu diene, Nutzer_innen über die effektiven Nutzungsbedingungen aufzuklären.

Das umfangreiche Datensammeln von Unternehmen habe es als eine doppelte Problematik den Geheimdiensten leichter gemacht, an Überwachungsdaten zu gelangen, da letztere sich die gewünschten Daten aus den zentralen Beständen der Unternehmen abgreifen könnten, obgleich dies nach aktuellem Kenntnisstand nicht unbedingt in Kooperation mit den Unternehmen geschehe. Demnach habe ein hinsichtlich seiner Datenerfassungsverfahren unkontrollierter Markt, der zudem auch freiwillig von Nutzer_innen mit Informationen gefüttert werde, die Informationsgewinnung der Geheimdienste massiv vereinfacht.

3. Mangelnde Spürbarkeit von Überwachung

Systeme und Geschäftsprozesse des digitalen Zeitalters seien in ihrer Komplexität für die breite der Bevölkerung undurchschaubar. Die beschriebene Intransparenz dieser komplexen Systeme führe zu einer Kapitulation der Verbraucher_innen vor der Auseinandersetzung, die Erfassung ihrer persönlichen Daten einzuschränken.

Begünstigt werde diese Kapitulation durch eine Unkenntnis über den eigentlichen Wert der gesammelten Informationen, die oft auch als das Gold des 21. Jh. bezeichnet würden. Es sei individuell schwer fassbar, welchen finanziellen Gegenwert eine Information wie die eigene Adresse habe, sodass die Herausgabe dieser für eine bestimmte Dienstleistung zu einem Vertrag führe, bei dem ein Gespür darüber, ob die Zahlung mit einer bestimmten personenbezogenen Information für die gewünschte Dienstleistung einen adäquaten Gegenwert darstelle, verloren gehe.

Mangelnde Spürbarkeit von Überwachung beruhe auf der bisher nicht feststellbaren nachteiligen Betroffenheit durch Überwachung für die Verbraucher_innen, bspw. im Hinblick auf höhere Preise durch kommerzielle Überwachung oder Verwehrung eines Dienstes aufgrund negativer Nutzer_inneneinstufung.[34]

Eine gängige Schlussfolgerung der Nutzer_innen aus der Feststellung mangelnder Betroffenheit sei jene, nichts zu verbergen zu haben. Dies geschehe unter der Annahme, die Herausgabe einer persönlichen Adresse oder das Verfassen eines Online-Beitrages sei folgenlos. Problematisch sei diese Auffassung, da sie die Dimension an negativen Folgen nicht kalkuliere, die auf den komplexen Verknüpfungsmöglichkeiten einzelner, isoliert betrachtet kaum belastender Informationspartikel beruhe, wodurch Informationsbilder ermöglicht würden, die in ihrem Detailreichtum kaum im ursprünglichen Sinne der Nutzer_innen gewesen wären.

Das von staatlichen Überwachungsorganen vorgebrachte Sicherheitsargument, Überwachung sei bspw. im Sinne der Terrorprävention nötig, führe zu einer Duldung von Überwachung. Versprochener

34 Anm. d. Pr.: Eine Studie, die u. a. individuelle Preisanpassungen aufgrund der aus kommerzieller Überwachung gewonnen Nutzer_innendaten nachweist, erschien im Nov. 2014: WOLFIE, C.: „Kommerzielle digitale Überwachung im Alltag“, Studie von Cracked Labs im Auftrag der österreichischen Bundesarbeitskammer, 2014, online abrufbar unter: http://crackedlabs.org/studie-kommerzielle-ueberwachung/info (zuletzt aufgerufen: 02. Okt. 2015).

staatlicher Schutz gegen mögliche Terrorangriffe sei so ein akzeptabler Gegenwert für die Überwachung.

Ein weiteres Problemfeld sei die Aufforderung an Verbraucher_innen, für den Schutz ihrer Daten selbst Sorge tragen zu müssen. Ein steigendes Bewusstsein für Datenschutz sei durchaus in der zunehmenden Nutzung der Privatsphäre-Einstellungen sozialer Netzwerke feststellbar, zu Beobachten bspw. am Nutzer_innenverhalten des sozialen Netzwerkes studiVZ seit dem Jahr 2009. An der aktuellen Selbstverständlichkeit der Verwendung von Virenscannern und komplexeren Passwörtern lasse sich der Wille von Verbraucher_innen erkennen, für den Schutz ihrer digitalen Daten einzutreten. Der Wunsch, Informationen nur in geschützten Räumen auszutauschen, sei bspw. auch am Verhalten Jugendlicher ersichtlich, die ein Interesse daran hätten, ihre Äußerungen in sozialen Netzwerken vor den Blicken der Eltern zu verbergen. Problematisch sei das Verständnis von der Beschaffenheit eines solchen geschützten Raumes, da viele Verbraucher_innen einem virtuellen Raum, der lediglich mittels bestimmter Zugangsdaten betreten werden könne, automatisch den Status eines geschützten, also nicht-öffentlichen Raumes beimäßen. Aus der Kollision dieser Raumempfindung mit der Erkenntnis, von Geheimdiensten und Dienstanbietern jener scheinbar geschützten Räume ausgespäht zu werden, entstehe zumindest ein empfindlicheres Bewusstsein für das Thema Datenschutz.

Eine Errungenschaft großer Anbieter wie Google und Facebook sei die Förderung einer gleichgültigen Einstellung von Verbraucher_innen hinsichtlich der Herausgabe ihrer persönlichen Daten für einen sehr komfortabel zu benutzenden Dienst. Der empfundene Mehrwert jener Dienste übersteige den empfundenen Wert der dafür herausgegebenen Informationen. Dieser Umstand müsse trotz all seiner innewohnenden Problematik unter dem Aspekt eines Selbstbestimmungsrechtes der Nutzer_innen anzuerkennen sein.

4. Aufklärung und gesetzlicher Schutz

Aus der Sicht des Verbraucher- und Datenschutzes sei es unumgänglich, die Komplexität der Überwachung durch Unternehmen und Geheimdienste vom Abstrakten ins Konkrete zu überführen. Nötig sei dies, da sich aus Sicht der Arbeit des Verbraucherschutzes bis zum aktuellen Tag kein Unterschied im Nutzer_innenverhalten in der Zeit vor und nach den Snowden-Enthüllungen feststellen lasse. Sehr deutlich werde eine Gleichgültigkeit den Snowden-Enthüllungen gegenüber auch an den sinkenden Zahlen der “Freiheit statt Angst”-Protestbewegungen.[35] Dieser Umstand sei aus der Abstraktheit der Überwachungsthematik zu erklären, die keine Betroffenheit der Verbraucher_innen auslöse.

Ein erster Ansatz zur Auflösung dieser Abstraktheit bestehe in der Aufklärung darüber, den Informationsgehalt einer einzelnen digitalen Auskunft durch die umfangreichen Verknüpfungsmöglichkeiten dieser Informationen zur Profilerstellung nicht zu unterschätzen. Ein zweiter Ansatz sei die Distanzierung von Schuldzuschreibungen der Art, Verbraucher_innen hätten die möglichen Missbräuche von Überwachung selbst zu tragen, wenn sie digitale Daten preisgäben. Ein

35 http://freiheitstattangst.de/ (zuletzt aufgerufen: 02. Okt. 2015).

Schutz von Verbraucher_innen müsse allgemeingültig auch im digitalen Raum gegeben sein, ohne diesen Schutz zuvor selbst einfordern zu müssen.

In diesem Zusammenhang sei zu beachten, dass menschliches Dasein mit der Herausbildung individueller Rollen einhergehe und das Ausleben dieser bewusst voneinander getrennten Rollen, bspw. einer privaten und einer öffentlich-beruflichen, einem Schutz vor Überwachung unterliegen müsse.

Ziel der Datenschutzdebatte könne nicht sein, Bürger_innen lediglich in digitaler Selbstverteidigung auszubilden, da in einem demokratischen Staat auch der Schutz des digitalen Raumes zum Aufgabenbereich des Staates gehöre.

Eine Eingrenzung der Datensammlung von Unternehmen sei ein wichtiges politisches Ziel, welches bereits in der europäischen Datenschutzverordnung verfolgt werde. Eine positive Begleiterscheinung gesetzlicher Datenschutzregulierungen wäre der indirekte Schutz vor der Datensammlung durch Geheimdienste, sofern die Möglichkeit für Verbraucher_innen entstehe, mit zu entscheiden, auf welche Art Daten gesammelt würden und wie lange diese vorgehalten werden dürften. Informationen, die nicht mehr vorgehalten würden, könnten schließlich auch nicht an Geheimdienste weitergeleitet werden.

Eine qualitative Aufbereitung der Informationen zum Datenschutz und der Privatsphäre für Verbraucher_innen sei der einer quantitativen Häufung von Informationen, die aktuell zu beobachten sei, vorzuziehen. Ein vielversprechender Ansatz dafür sei, Verbraucherschutzinformationen durch bestimmte, schnell erfassbare Symbole zu vermitteln. Technische Expertise hinter Überwachungsmechanismen sei ebenso dafür einsetzbar, auf hohem Standard für den Schutz von Verbraucher_innen zu sorgen. Beispiele für Ansätze auf europäischer Ebene seien Privacy by Design (“Schutz der Privatsphäre als Teil der Konstruktion”) und Privacy by Default (“Auf den Schutz der Privatsphäre hin eingerichtete Voreinstellungen”), welche die Herausgabe von Daten in den Grundeinstellungen verhindere und diese erst durch aktives Eingreifen der Verbraucher_innen ermögliche sowie das Konzept, Datenschutz als festen Bestandteil von Produktkonstruktionen zu sehen.

Ein Zusammenspiel von gesetzlichen und technische Lösungen sowie Aufklärung und Transparenz könnten in einigen Jahren dazu führen, eine Datenhoheit für Verbraucher_innen zurückzugewinnen. Die Forderung nach Transparenz müsse auch in Richtung der bisher kaum vorhandenen Erforschung der unterschiedlichen Verbrauchertypen hinsichtlich ihrer Kompetenzen über den digitalen Raum erfolgen, um fundierte Erkenntnisse darüber zu gewinnen, wie Verbraucher_innen Informationen wahrnähmen und aufnähmen. Erst dadurch könne Aufklärungsarbeit in einem Maße wirken, Verbraucher_innen zu einem bewussteren Umgang mit der Privatsphäre zu befähigen. Erst eine kompetente Auseinandersetzung der Verbraucher_innen könne eine wirklich bewusste Entscheidung für und wider die Preisgabe ihrer Daten ermöglichen. Ziel sei eine kompetente Selbstbestimmung von Verbraucher_innen, keine Fremdbestimmung.

Offene Diskussion der Gastvorträge

Abkürzungen der Namen:
MZ: Michaela Zinke
FW: Florian Wobser
TG: Tom Gehrke
Mod. AK: Amon Kaufmann (Moderation)
RH: Roland Hummel (Protokoll)

Nach einer zehnminütigen Pause erfolgte unter der Moderation von Amon Kaufmann (AK) die offene Diskussion der Gastvorträge. Für Fragen zur Überwachungsprävention lud AK zu den praktischen Teilen der Veranstaltungsreihe ein, in denen ein adäquater Diskussionsraum für diese besonderen Problematiken bestehe. Ebenso verwies AK auf den FAZ-Artikel “Whistleblower Edward Snowden – Der hat doch gar nichts enthüllt”[36], welcher zur bereits angesprochenen Problematik um die fehlende direkte Betroffenheit durch die Überwachung beitrage.

Mit einem Appell, Überwachung nicht die Meinungsäußerung beeinträchtigen zu lassen, wurde die Diskussion eröffnet:

Mod. AK: In dem eingespielten Videoausschnitt mit Sarah Harrison wurde der Umstand problematisiert, dass durch geheimdienstliche Arbeit die persönlichen Daten normaler Bürger_innen öffentlich, die Daten von öffentliche Amtsträgern jedoch geschützt seien. Wie sei dieser Umstand zu beurteilen und sollte alles, was zum politischen Amt einer Person gehört, öffentlich sein?

Hörer_in: Das Private einer politischen Person sollte selbstverständlich privat bleiben, ihre Tätigkeiten in politischer Funktion müssten jedoch für die Öffentlichkeit zugänglich sein.

TG: [an Vorredner_in] Rückfrage, warum dies seiner/ihrer Ansicht nach so sein müsse.

Hörer_in: [an Vorredner_in] Mangelnde Transparenz der konkreten Arbeitsweise staatlicher Institutionen, deren Macht vom Volk gegeben sei, wäre Ausdruck einer mangelhaften Demokratie.

TG: [an Vorredner_in] Rückfrage, ob demnach aktuell eine mangelhafte Demokratie festzustellen sei.

Hörer_in: [an Vorredner_in] Bejahte die Frage. Vor allem sei dies dem Umstand zu verantworten, dass Instanzen wie Informationsmedien, ihrer Aufgabe zur Aufklärung nicht ausreichend nachkämen bzw. nicht ausreichend nachkommen könnten.

Hörer_in: Gegen eine völlige Transparenz der Arbeitsweise staatlicher Organe spräche vor allem die Gefahr einer drohenden Lynchjustiz, wäre bspw. die Arbeit der Judikative völlig öffentlich. Lynchjustiz sei höchst demokratisch und absolut grausam zugleich. Die Geschichte zeige viele Versuche, eine optimale Regierungsform zu finden. In diesem Zusammenhang sei der Kreis der vorgestellten Philosophen durch Aristoteles zu erweitern. Wichtig sei, dass der heutige Umstand einer relativ sicheren Gesellschaft der Entwicklung einer zweitausendjährigen Geschichte bedurft habe. Aus der Analyse des Verbraucherschutzes sei deswegen die Verantwortung der Verbraucher_innen hervorzuheben. Daneben sei im Zusammenhang mit dem Recht auf Privatsphäre als Eigenschaft des menschlichen

36 MICHAL, W.: „Whistleblower Edward Snowden - Der hat doch gar nichts enthüllt“, faz.net, 10. Jun 2014, online abrufbar unter: http://www.faz.net/aktuell/feuilleton/whistleblower-edward-snowden-der-hat-doch-gar-nichts-enthuellt-12982298.html – Kurzlink: http://www.faz.net/-gqz-7q97e (zuletzt aufgerufen: 02. Okt. 2015).

Charakters sein Wille zum öffentlichen Auftreten festzuhalten. Die aktuelle Debatte sei ein Kulturkampf, der analog zur 68er-Bewegung zu bewältigen sei.

TG: [an Vorredner_in] Rückfrage, wie genau diese Bewältigung stattfinden solle.

Hörer_in: [an Vorredner_in] In Form einer Entwicklung durch Diskussionen und Gesetze. Sicherzustellen sei, dass auch große Unternehmen staatlich hinsichtlich ihrer Überwachungspraktiken kontrolliert werden dürften. Edward Snowden solle für den Anstoß der aktuellen kulturellen Entwicklung den Friedensnobelpreis bekommen. Problematisch wäre auf Seiten der Bürger_innen der Verzicht auf Vorzüge der globalen Vernetzung wie Preisvergleichsportale, die für jede Dienstleistung das günstigste Angebot herausfiltern, da die derzeitig gewünschten Regulierungen auf solche Vorteile wie eine Diktatur wirken würden, beginnend mit der Frage, wer die Rolle des Regulierers übernehmen solle. Die aktuelle Debatte hebe sich von denen der menschlichen Geschichte nur durch ihre neue kulturelle Stufe ab, die es in optimistischer Weise zu bewältigen gelte, vor allem durch Diskussionen wie die aktuelle.

Hörer_in: Politisches Handeln solle in jedem Fall transparent sein. Die für die Öffentlichkeit intransparenten Verhandlungen zum geplanten Freihandelsabkommen[37] seien ein Beispiel für undemokratische Verhältnisse, da in diesem Zusammenhang über ein Gesetz entschieden würde, über dessen Vor- und Nachteile zuvor keine Meinungsbildung für die Öffentlichkeit möglich sei.

Hörer_in: Die Beschäftigung mit dem Freihandelsabkommen sei von hoher Bedeutung, da ein entsprechendes Abkommen mit den USA sich auch immens auf bestehende Datenschutzverhältnisse auswirke. Lobbyarbeit der USA wirke sich in ihrer Stärke zu Ungunsten des deutschen und europäischen Marktes sowie auf Regelungen des Verbraucherschutzes aus. Daneben müssten Institutionen wie Kartellämter dafür Sorge tragen, die Monopole von Internetgiganten zu brechen. Die Marktmacht dieser Unternehmen ermögliche es ihnen, sich beständig weitere Technologien einzukaufen, die von Bürger_innen täglich genutzt werden, sodass die Abhängigkeit von diesen Unternehmen immer mehr zunehme. Demzufolge müssten Monopolstellungen gebrochen und Politiker_innen (wie Sigmar Gabriel in Bezug auf seine Bemühungen zur Durchsetzung des Freihandelsabkommens) stärker beobachtet werden.

Hörer_in: Problem der Bürger_innen sei nicht, über zu wenige Informationen zu verfügen, sondern im Gegenteil kaum noch Informationen wahrnehmen zu können. Festzustellen sei, dass ein Großteil der Bürger_innen sich kaum mit klassischen Printmedien wie Wochenzeitungen auseinandersetze. Zugleich würden durch unterschiedlichste Verbände in der bürgerlichen Medienlandschaft täglich neue Veröffentlichungen inoffizieller staatlicher Dokumente publiziert (Whistleblowing). Das Gefühl eines Informationsmangels und einer intransparenten Gesellschaft sei hinsichtlich der Informationsflut absurd. Ebenso sei die Vorgehensweise von Enthüllungsplattformen wie WikiLeaks, die alle Informationen ungefiltert veröffentlichten, anzuzweifeln. Es mangele auf jeden Fall nicht an Informationen, vielfältige Angebote der Internets wie soziale Netzwerke lenkten jedoch von den verfügbaren Informationen ab.

37 Anm. d. Pr.: Gemeint war die „Transatlantische Handels- und Investitionspartnerschaft“ bzw. „**T**ransatlantic **T**rade and **I**nvestment **P**artnership”.

Der Referentin Michaela Zinke sei in ihrer Aussage zu widersprechen, der Staat sei auf verschiedenen Ebenen für den Schutz der Bürger_innen in seine Verantwortung zu ziehen. Vielmehr habe jedes Individuum die Freiheit, sich bspw. durch eigene Auswahl seiner Internetdienstleister selbst zu schützen. Das Scheitern der Bürger_innen in Bezug auf Überwachung erfolge in gleichgültiger, aber durchaus bewusster Art und Weise darüber, in der täglichen Benutzung datenschutzproblematischer Dienste einen Fehler zu begehen.

[Zuspruch aus der Hörer_innenschaft]

Hörer_in: Auffallend sei in den bisherigen Beiträgen eine Doppelmoral, umstrittene Internetdienste zu verurteilen, sie aber gleichzeitig zu benutzen. Der/die Hörer_in merkte an, Dienste wie Google und Facebook mit Begeisterung persönlich einzusetzen. Die komfortable Möglichkeit gemeinschaftlichen Arbeitens mit Google Drive sei hervorzuheben. Konzerne wie Google hätten solch komfortabel zu benutzenden Dienste erst möglich gemacht.

Hörer_in: Zusätzlich zur Diskussion um die Frage nach der Transparenz öffentlicher Ämter solle die Frage gestellt werden, wie es um die Transparenz öffentlicher Handlungen von Privatpersonen bestehe. Es stelle sich die Frage, ob die Teilnahme an einer klassischen Demonstration auf der Straße als Form einer öffentlichen Meinungsäußerung einer Meinungsäußerung in einem sozialen Netzwerk gleichkomme. Zu beobachten sei die Ansicht, soziale Netzwerke ermöglichten ihren Nutzer_innen öffentliches Handeln. Zu diskutieren sei die Frage nach der Sinnhaftigkeit dieser Möglichkeit.

Hörer_in: Der Datenflut des Internets sorge wie nie zuvor für Möglichkeiten, sich zu informieren. Es mangele jedoch an einer Verknüpfung dieser Wissensressourcen, um sie nutzbar zu machen. Verknüpfungskonzepte würden helfen, Zusammenhänge zwischen den Informationen herzustellen.

Daneben sei es unbegreiflich, dass Edward Snowden nach wie vor lediglich in Russland Zuflucht finde und ein deutlicher Protest der Bevölkerung vor dem Kanzleramt ausbleibe, um daran etwas zu ändern. Dies auch im Zusammenhang des NSA-Untersuchungsausschusses, der Edward Snowden als Kronzeugen nicht einlade. Dieser Zustand sei nicht einem Informationsmangel über die Person Edward Snowden zuzuschreiben, sondern vielmehr einem Mangel an Informationen über die konkreten Inhalte seiner Enthüllungen.

MZ: [auf den Beitrag zum Thema „Kartellämter"] Das Kartellrecht ermögliche aktuell nicht die Reglementierung von Internetunternehmen. Dies läge vor allem an der Problematik der Klassifizierung eines Unternehmens wie Google, welches in unterschiedlichsten Geschäftsfeldern tätig sei und selbst in diesen einzelnen Geschäftsfeldern Monopole innehabe, wodurch eine Aufspaltung dieses Unternehmens am status quo nichts ändere. Das Kartellrecht ließe sich als reglementierendes Instrument nur durch eine vorangehende Reform desselben wirksamer einsetzen. Mit einer solchen Reform sei in absehbarer Zeit kaum zu rechnen.

[Auf die angesprochene Problematik des Informationsüberflusses] Hinzukomme die Problematik, dass die Veröffentlichung nicht-öffentlicher Dokumente bspw. zum Freihandelsabkommen oder der EU-Datenschutzverordnung im Rahmen der EU-Ratsverhandlungen inhaltlich zum Zeitpunkt ihrer

Veröffentlichung oftmals bereits so veraltet seien, dass eine wirksame Reaktion durch Aktivist_innen darauf kaum mehr möglich sei.

[Auf den Einwand, der Staat stehe nicht in der Verantwortung zum Schutz der Bürger_innen] Der Reformprozess gegen Überwachung sei ein sehr langer, der auf jeden Fall auf staatlicher Seite stattfinden müsse, jedoch auch eine Verhandlung unter den Bürger_innen einer Gesellschaft sei. Das Verständnis über den Raum des Privaten müsse demnach auch innergesellschaftlich neu verhandelt werden. Bedeutend sei aktuell die Feststellung eines nicht regulierten Marktes im Internet, der reguliert werden müsse. Es reiche nicht, Bürger_innen lediglich persönliche Instrumentarien zu liefern, ihre Privatsphäre eigenständig zu schützen. Ein wirksamer, eigenständiger Schutz sei höchstens einem entsprechend geschulten Teil der Bevölkerung möglich. Ein Großteil der Bürger_innen sei faktisch für den Schutz der Privatsphäre auf den Staat angewiesen, indem dieser für den Datenschutz bei der Benutzung von Internetdiensten gesetzlich Sorge trage.

Hörer_in: Eine wirklich sichere Kommunikation im Internet könne nicht durch Gesetze erreicht werden. Statt der Frage nach einem Protest der Bevölkerung vor dem Kanzleramt sei die Nutzung von wirksamer E-Mailverschlüsselung durch die Bevölkerung von größerer Bedeutung.

Hörer_in: [an Vorredner_in] Rückfrage, warum eine gesetzliche Vorschrift zur Verschlüsselung nicht möglich sei.

Hörer_in: Der Umstand, dass selbst die Bundeskanzlerin über kein abhörfreies Telefon verfüge untermauere die fehlende Kompetenz des Staates, für sichere Kommunikation sorgen zu können. Läge die Verschlüsselung von Kommunikation in der Hand des Staates so obläge diesem dann zudem die Wahl eines Verschlüsselungsverfahrens, in dessen korrekte Handhabung durch den Staat ich vertrauen müsse. Garantiert vertrauliche Kommunikation sei momentan nur durch Eigeninitiative möglich. Im Vergleich zur überaus komfortablen Handhabung von Google-Produkten würden diese Eigeninitiative die wenigsten Bürger_innen auf sich nehmen.

Alternativen etablierter Internetdienste wie bspw. die auf Datenschutz ausgelegte Suchmaschine DuckDuckGo würden im Vergleich Google als eine leistungsfähigere Suchmaschine verdeutlichen.

Mod. AK: [an Vorredner_in] Anmerkung, DuckDuckGo sei im Grunde Google.

Hörer_in: [fortführend] Aus diesem Grund werde ein Großteil der Bevölkerung nie eine andere Suchmaschine nutzen als Google und es nie als Problem empfinden, für die Leistung sehr guter Suchergebnisse private Informationen an Google zu liefern. Im Gegenteil würden diese privaten Informationen die Suchergebnisse von Google weiter verbessern. Daraus ergebe sich das Problem, dass eine gesetzliche Einschränkung der Datensammlung von Unternehmen schlechtere Dienstleistungen dieser Unternehmen zur Folge hätte. Aus der gleichgültigen Haltung der Bevölkerung den Datensammelpraktiken der Unternehmen gegenüber ergebe sich die Frage, ob eine gesetzliche Vorschrift bspw. zur E-Mail-Verschlüsselung nicht nur bei den Unternehmen, sondern vor allem bei den Bürger_innen überhaupt durchsetzbar sei.

Hörer_in: Eine Nutzung des Internets frei von möglichen Gefahren sei nicht möglich, ungeachtet der Kompetenz der Nutzer_innen. Gefahren bestünden zu jedem Zeitpunkt in der realen wie virtuellen Welt.

Eine Gefahrenprävention im virtuellen Raum durch staatliche Regulierung ziehe weitreichende Probleme nach sich. In der Umsetzung einer solchen Regulierung ergebe sich nämlich sowohl auf wirtschaftlicher als auch auf sozio-kultureller Ebene die Frage, von welcher Instanz aus diese erfolgen solle, da das Internet ein internationaler Raum sei. Regulierung käme einer Zensur, ähnlich in Russland und in China, gleich, die in der westlichen Welt allgemeine Ablehnung fände.

Im Zusammenhang mit dem wenig beachteten Bericht des Europäischen Parlaments über das Abhörsystem „Echelon“[38] aus dem Jahre 2001 sowie der Problematik des Einsatzes der Rasterfahndung in Deutschland sei momentan eine Wiederholung der Überwachungsdebatte festzustellen, in welcher Desinteresse seitens der Bevölkerung eine Konstante sei. Diese Debatte beinhalte absurde Versuche, mittels ideologischer Programme viel zu komplexe Gegenwehrszenarien zu entwickeln, bspw. mit der Idee, durch Aufklärung und der Hoffnung auf eine positive Kettenreaktion der Bevölkerung E-Mail-Verschlüsselung beizubringen. Gegenwehrmaßnahmen müssten ohne staatliche Regularien allgemeinverständlich umsetzbar sein.

Mod. AK: Die Art und Weise der Veröffentlichung ursprünglich nicht für die Öffentlichkeit bestimmter Informationen durch Enthüllungsplattformen wie WikiLeaks zeige auch das Problem einer medienwirksamen Inszenierung solcher Informationen entgegen ursprünglicher Veröffentlichungsphilosophien. Dies werde am Beispiel des Videos „Collateral Murder“ deutlich, einem Zusammenschnitt von Luftangriffen durch Kampfhubschrauber US-amerikanischer Streitkräfte in Bagdad am 12. Jul. 2007, die u. a. auch auf Zivilisten erfolgten.[39] Diese Problematik müsse bei der Aufbereitung und Bereitstellung von Informationen mit bedacht werden.

FW: Die Festschreibung bestimmter Standards, bspw. Verfahren zur Absicherung der E-Mail-Kommunikation, berge die Gefahr, Nutzer_innen ein Gefühl von Sicherheit zu vermitteln, die nicht vorhanden sei. Dies werde an der umstrittenen Initiative „E-Mail made in Germany“ deutlich, deren System aber bei genauer Betrachtung, anders als suggeriert, keine Ende-zu-Ende-Verschlüsselung von E-Mails gewährleiste. Initiativen wie diese verdeutlichten die Notwendigkeit eines mündigen Umgangs mit Technologien, der gesetzlich nicht verordnet werden könne. An den bisherigen Beiträgen werde ein Spannungsfeld deutlich, welches sich um die Frage drehe, ob Datenschutz „von oben“ oder „von unten“ bzw. aus beiden Richtungen und in welchem Maß erfolgen müsse. Der These der Notwendigkeit einer digitalen Aufklärung sei zuzustimmen. Unter Bezug auf das Aufklärungsmodell Immanuel Kants sei es paradox, sich darauf zu verlassen, von staatlicher Seite aufgeklärt zu werden, da der Staat in diesem Zusammenhang auch in der Rolle des Überwachers stecke.

Mod. AK: Mangelnde Verschlüsselung in etablierten Technologien, zu denen auch das gesamte Telefonnetz gehöre, müssten leider an anderer Stelle diskutiert werden.

---

38 SCHMID, E.: „Abhörsystem »Echelon«“, Pressebericht des Europaparlamentes A5-0264/2001 vom 05. Sep 2001, online abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?type=PRESS&reference=DN-20010905-1&format=XML&language=DE#SECTION1 – Kurzlink: http://kurzlink.de/YvoHYlXJo (zuletzt aufgerufen: 02. Okt. 2015).

39 WIKILEAKS: „Collateral Murder“, 5. Apr. 2010, online abrufbar unter: https://wikileaks.org/wiki/Collateral_Murder,_5_Apr_2010 (zuletzt aufgerufen: 02. Okt. 2015).

FW: Spannend sei die sich momentan in der Diskussion abzeichnende Klammer der philosophischen Perspektive auf der einen und konkreter Handlungsfragen aus dem Alltag auf der anderen Seite, in der die Bedeutung von Autonomie von Verbraucher_innen wie sie Michaela Zinke in ihrem Vortrag unterstrich, hervorgehoben werden müsse. Ebenso sei ein Zustand der Orientierungslosigkeit hinsichtlich der Art und Weise einer wirksamen Reaktion auf die Überwachungsaffäre festzustellen. Ein Zustand der Ahnungslosigkeit über die Effektivität unterschiedlichster Maßnahmen (offener Protest, Verschlüsselung) bestimme den Diskurs. Nachhaltige Lösungen würden vor allem durch Momente erschwert, in denen sich mühevolle Veränderungen im Nutzer_innenverhalten, beispielsweise durch Verwendung komplexerer Passwörter, im Nachhinein als nutzlos herausstellten.

Hörer_in: Es müsse eine höhere Kontrolle in Unternehmen geben, die schon vorhandenen deutschen Gesetze konsequent umzusetzen. Dies sei bei amerikanischen Unternehmen mit ihren gänzlich anderen Vorstellungen von Privatsphäre nicht möglich, auch durch gesetzliche Umstände bedingt durch den Patriot Act. Es sei zu diskutieren, ob nicht vorhandene Gesetzgebung zumindest auf nationaler Ebene erlaube, eine tiefgreifende Kontrolle von Unternehmen hinsichtlich des Datenschutzes umzusetzen.

Hörer_in: [an FW] Entgegen einer Orientierungslosigkeit würden die Problemfelder der Vorträge, nämlich die Bereiche „privat“ und „öffentlich“, sehr klar aufgegriffen, indem aktuell besprochen werde, welche Handlungsoptionen für Verbraucher_innen und in Bezug auf Konzerne bestünden und wie das Verhältnis zwischen diesen Ebenen beschaffen sei. Die Brücke der inhaltlich äußerst unterschiedlichen Vorträge bestehe eventuell in der Thematisierung von Widerstand, der sich in der philosophischen Ebene aus der Gefährdung des Privaten im eingangs vorgestellten Rautenmodell ableiten lasse und auf der Ebene des Verbraucherschutzes aus der Konsequenz, Unternehmen einer stärkeren Kontrolle zu unterwerfen. Daraus ergebe sich erstens die Frage, auf wen konkret sich dieser Widerstand beziehen solle.

Eine zweite Frage beziehe sich inhaltlich auf den Vortrag von TG und FW. Ein übergreifendes Thema des philosophischen Vortrages sei die Veränderung von gesellschaftlicher Moral gewesen, die eine Selbstüberwachung in die Bürger_innen installiere. Die Haltbarkeit dieser These sei zum einen in Bezug auf einige der genannten Philosophen anzuzweifeln, zum anderen nicht vereinbar mit dem persönlichen Empfinden als bekennende(r) Christ_in, da die Moralinstanz in diesem Fall kein inneres Gespräch sei, sondern ein Bezug auf eine transzendente Ebene. Moralische Selbstkontrolle und Selbstzensur werde daher selten wahrgenommen [Anm. d. Pr.: Fragesteller_in bezog diese Feststellung auf sich selbst].

TG: [an Vorredner_in] Rückfrage, was an den Ausführungen zu „Foucault“ und „Pastoralmacht“ gestört habe sowie die Rückfrage, ob das thematisierte innere Gespräch bei ihm/ihr nicht bestehe und deshalb die Wirkung eines Machtmechanismus verneint werde.

Hörer_in: [an Vorredner_in] Es sei nicht klar geworden, wer die Macht in Bezug auf die Selbstkontrolle und Selbstzensur ausübe.

TG: [an Vorredner_in] Foucault sei so zu verstehen, dass der Machtmechanismus nicht durch Vermittler wirke, sondern durch vorfindliche Strukturen der Gesellschaft. Dieser Machtmechanismus einer

beständigen inneren Selbstthematisierung sei nach Foucault nicht bewusst wahrnehmbar. So würden die Auswirkungen der Pastoralmacht sich auf einer Ebene abzeichnen, die einer bewussten Reflexion entzogen sei.

FW: [an Vorredner_in] Der eigene Vortrag sei auf ein Panorama für Diskussionsimpulse ausgerichtet gewesen, wodurch die Einnahme persönlicher Positionen weniger Raum gehabt habe. Daraus ergebe sich das Problem des Bezuges auf konkrete Probleme wie das zuvor angesprochene Problem, wenn ein(e) Hörer_in als bekennende(r) Christ_in die Wirkung einer Pastoralmacht abstreite. Diese Auffassung sei aus persönlicher Sicht von TG und FW abzustreiten, es läge aber nicht im Interesse von TG und FW, der versammelten Hörer_innenschaft vorzuhalten, sie unterläge der Kontrolle einer Pastoralmacht. Ziel sei ein Referat gewesen, welches u. a. Foucaults Position wiedergebe, die selbstverständlich kritikfähig sei. Der in der Eröffnung von RH angesprochene Topos der Verschwörungstheorie sei TG und FW bereits in der Vorbereitung im Bewusstsein gewesen, sodass der Vortrag darauf ausgerichtet worden sei, keine Verschwörungstheorien zu entwickeln oder zu bedienen. Es ergebe sich jedoch die Frage, ob im aktuellen gesellschaftlichen Diskurs überhaupt noch außerhalb von Verschwörungstheorien gedacht werden könne.

[Zuspruch aus der Hörer_innenschaft]

MZ: [auf die These, Regulierung käme einer Zensur gleich] Rückfrage, warum es einer Zensur gleichkäme, Unternehmen im Sammeln von Nutzer_innendaten gesetzlich einzuschränken.

Hörer_in: [an Vorredner_in] In China und Russland würde die Argumentation, die staatliche Regulierung legitimiere, analog der Argumentation von MZ ablaufen. Nationalstaaten hätten hinsichtlich ihrer jeweiligen Entwicklung unterschiedlichste Vorstellungen im Umgang mit dem Raum des Privaten entwickelt, daher sei der genannten These zu widersprechen, deutsche Regeln für den Datenschutz allgemein einzuführen. Facebook sei bspw. ein US-amerikanisches Produkt und entstamme damit einer Gesellschaft, zu der die deutsche in Bezug auf die allgemeine Auffassung von Menschenrechten einen engeren Bezug habe als bspw. zur chinesischen Gesellschaft. Gleichwohl gäbe es jedoch in gewissen Punkten, bspw. der Todesstrafe, gänzlich andere Auffassungen im Umgang mit Menschenrechten. Jeder Staat entwickele seine individuellen Vorstellungen im Umgang mit Menschenrechten, so auch in Bezug auf den Umgang mit der Privatsphäre. Die Idee der Einigung auf globale Gesetzgebungen zum Datenschutz sei zu begrüßen, um dem Missbrauch digitaler Netze entgegenzuwirken. Andererseits würden die durchaus vorhandenen Kehrseiten eines nicht regulierten Internets oftmals zur Argumentation herangezogen, die freie Nutzung des Internets einzuschränken. Die Häufigkeit, mit der bspw. die Problematik um Kinderpornographie in öffentlichen Diskursen erwähnt werde, erzeuge ein Bild einer Gesellschaft bestehend aus Pädophilen. Kriminelle fänden auch durch gesetzliche Regularien hindurch Wege, das Internet zu missbrauchen. Für Normalbürger_innen hingegen bedeute eine Regulierung des Internets eine permanente Einschränkung, die sowohl durch staatliche Forderungen als auch durch Forderungen von Datenschützer_innen entstünden. Der Raum des Internets müsse ein anarchistischer bleiben.

MZ: [an Vorredner_in] Rückfrage, ob das Internet momentan tatsächlich ein anarchistischer Raum sei.

Hörer_in: [an Vorredner_in] Feststellung, dass das Internet aktuell zumindest kein regulierter Raum sei.
MZ: [an Vorredner_in] Ablehnung der These. Wolle aber ein US-amerikanisches Unternehmen ein Produkt in Deutschland verkaufen müsse das Produkt lokale Gesetze einhalten. Unter wirtschaftlicher Betrachtung sei das Internet ebenso in nationale Märkte aufgeteilt. Entsprechend stelle sich die Frage, warum nationale Datenschutzregelungen der realen Welt nicht auch für die virtuelle als Kriterium herangezogen werden könnten, wolle ein Unternehmen eine virtuelle Dienstleistung bspw. auf dem deutschen Markt anbieten.
Hörer_in: [an Vorredner_in] Einwand, ein virtuelles Produkt werde, sofern es in den USA gekauft werde, durch den Standort der jeweiligen Rechnersysteme auch dort genutzt, nicht in Deutschland.
MZ: [an Vorredner_in] Einwand, das Produkt werde dennoch auf dem deutschen Markt und demnach in deutscher Sprache angeboten. Beim Verkauf ausländischer Produkte, die entsprechend im Ausland produziert würden, fände für den Verkauf auf dem deutschen Markt eine Anpassung entsprechend der deutschen Gesetzgebung statt. Regelungen dieser Art seien schwer erkämpfte Grundrechte, die verteidigt werden sollten.
Hörer_in: [an Vorredner_in] Widerspruch; der Staat solle Grundrechte für Bürger_innen nicht auslegen.
MZ: [an Vorredner_in] Einwand, der Staat trete für die Zusicherung dieser Grundrechte ein.
Hörer_in: [an Vorredner_in] Widerspruch; der These könne nicht zugestimmt werden.
Mod. AK: [an Vorredner_innen] Abbruch der punktuellen Debatte; nach Veranstaltungsende gäbe es Zeit und Raum für eine Fortsetzung.
Hörer_in: Ein neuer Diskussionsaspekt in Bezug auf kulturelle Fragen sei die Suche nach menschlichem Glück wie sie in Platons Politeia als Kriterium für die Ausrichtung einer Gesellschaft thematisiert werde. Diese gesellschaftliche Ausrichtung laufe auf Bildung der Gesellschaft hinaus sowie auf eine Leitung der Gesellschaft durch Philosoph_innen. Diese Denkweise sei allerdings eine europäische. Philosophien anderer Kulturkreise müssten im Zusammenhang der diskutierten Problematik das europäische Problembewusstsein keinesfalls teilen. Durch Technologien wie die des Internets wachse die Welt jedoch zusammen, bspw. in der flächendeckenden Verwendung der englischen Sprache, entsprechend verlören europäische Denkweisen auch eine gewisse Vormachtstellung. In diesem Prozess bestehe die persönliche Suche nach Glück als eine natürliche Konstante fort und berge, dies zeige die Debatte dieses Abends, entsprechende Divergenzen, deren zugrundeliegenden Fragestellungen sich durch die weltweite Vernetzung globalisierten. Ein globaler Konsens in diesen Fragen beinhalte die Gefahr, Ausdruck einer globalen Diktatur zu sein. Probleme der weltweiten Vernetzung seien ferner nicht durch deutsche Normen zu lösen, bedenke man das Zusammenwachsen unterschiedlichster Kulturkreise. Die aktuelle Debatte sei in historischer Linie gesellschaftlicher Problemlösungen seit der Antike zu sehen, bspw. der Diskussion um die beste Regierungsform wie im antiken Athen.
TG: [an Vorredner_in] Rückfrage, wie der Prozess einer Problemlösung einer antiken Volksversammlung auf eine globale Ebene zu überführen sei. Voraussetzung dafür sei ein gesetzlicher Rahmen und eine Mündigkeit der Entscheidungsträger.

Mod. AK: [an Vorredner_innen] Abbruch der punktuellen Debatte; aufgrund des Zeitrahmens der Diskussionsveranstaltung müsse an dieser Stelle das Wort an weitere Hörer_innen übergeben werden.

Hörer_in: [an TG] Ethik müsse in jedem gesellschaftlichen Wandlungsprozess neu verhandelt werden, getrieben vom Menschen auf der Suche nach Glück, Frieden und Sicherheit.

FW: [an Vorredner_in] Problematisch an dieser Position sei das damit entworfene Bild einer menschlichen Geschichte ohne Tragödien.

Mod. AK: [an Vorredner_innen] Die punktuelle Debatte müsse an dieser Stelle zugunsten weiterer Wortmeldungen beendet werden.

Hörer_in: Dem/der Vorredner_in aus der Hörer_innenschaft sei zu widersprechen, da die vorgestellten Thesen über den Ursprung der Demokratie einer westlichen Perspektive geschuldet seien, die global nicht konsensfähig seien.

Hörer_in: [an Vorredner_in] Einwand, der Widerspruch gebe eigentlich das verfolgte Anliegen wieder. Laotse habe andere Probleme als Sokrates.

Hörer_in: [an Vorredner_in] Einwand, es werde zu stark fokussiert.

Hörer_in: [an Vorredner_in] Einwand, es werde selbstverständlich aufgrund von Sprachbarrieren fokussiert, da bspw. die chinesische Sprache im Vergleich zur englischen keine gängige Fremdsprache sei.

Hörer_in: [an Vorredner_in] Der Einwand hätte sich auf die These gestützt, Englisch sei eine flächendeckend gesprochene Sprache.

Hörer_in: [an Vorredner_in] Einwand, dies sei durchaus der Fall, vergleiche man die Verbreitung der chinesischen mit der englischen Sprache.

Mod. AK: [Abbruch der punktuellen Diskussion]

Hörer_in: Zu reflektieren sei die These, deutscher Datenschutz sei qualitativ der beste. Zuzustimmen sei der These, das Internet müsse in seiner anarchistischen Struktur erhalten bleiben. Es ergebe sich die Frage, ob nach einem globalen Datenschutz nach deutschen Standards populäre Dienste wie das soziale Online-Nachrichtenportal reddit[40] noch möglich seien.

MZ: [an Vorredner_in] Das Internet sei kein rechtsfreier Raum. So greife für deutsche Internetnutzer_innen deutsches bzw. europäisches Recht, unter gewissen Umständen auch US-amerikanisches Recht, damit aber in jedem Fall immer ein Recht.

Hörer_in: [an Vorredner_in] Gemeint sei bspw. die Problematik einer Impressumspflicht, die für deutsche Internetseiten bestehe, für US-amerikanische jedoch nicht. Deutsches Recht schränke damit global eingesetzt die Möglichkeit ein, anonym zu bleiben.

Hörer_in: Eigenverantwortlichkeit sei ein wichtiger Punkt gegen das vorherrschende Gefühl einer selbstmitleidigen Machtlosigkeit, dennoch sei es legitim, vom Staat adäquaten Schutz einzufordern. Der Staat sei ein von den Bürger_innen selbst gegebenes System, das überflüssig werde, sofern es seiner Verantwortung den Bürger_innen gegenüber nicht nachkomme. In diesem Fall würden andere Formen der gesellschaftlichen Organisation notwendig werden.

40 https://www.reddit.com/ (zuletzt aufgerufen: 04. Nov. 2015).

TG: [an Vorredner_in] Rückfrage, ob in dieser Feststellung nicht durchaus eine angemessene Konsequenz der Überwachungsaffäre läge. [Zuspruch aus der Hörer_innenschaft] Dies sei nicht Ausdruck einer politischen Überzeugung, aber die Frage nach der Funktionstüchtigkeit der Demokratie sei berechtigt, sobald die Verlässlichkeit ihrer Prinzipien nicht mehr gegeben sei. Eine Verlässlichkeit für den Schutz vor Überwachung sei schwer durch Instanzen vorstellbar, die von Überwachung profitierten.

Hörer_in: [an Vorredner_in] Vorteile durch Überwachung hätten zunächst Unternehmen. Daneben gäbe es durchaus Bereiche, in denen staatl. Kontrolle zugunsten einer Gefahrenprävention gewisse Mindeststandards durchsetze. Im Bereich von Nahrungsmitteln sei so gewährleistet, dass Bürger_innen gefahrlos Produkte einkaufen könnten. Daraus ergebe sich eine Hoffnung der Verbesserung auch für andere Bereiche, angetrieben durch öffentlichen Druck. Die Möglichkeit zur Unkenntlichmachung der eigenen Wohnung im Online-Kartendienst Google Street View sei hier als positives Beispiel zu erwähnen.

MZ: [an Vorredner_in] Dieses Beispiel sei problematisch, da das rechtliche Verfahren dahinter sehr viele Möglichkeiten zur Auslegung biete, bspw. im Falle eines Antrages auf Unkenntlichmachung eines Mehrfamilienhauses durch nur eine Familie desselben.

Der These zur Impressumsproblematik sei zuzustimmen, jedoch hätten auch deutsche Nutzer einer Internetseite das Recht, diese vollständig anonym zu nutzen. Impressumspflicht gelte nicht für Besucher_innen einer Internetseite wie an Urteilen des Bundesgerichtshofs deutlich werde, durch welche die Herausgabe von personenbezogenen Daten unterbunden wurde, bspw. nach negativen Bewertungen von Mediziner_innen auf Bewertungsportalen durch Patient_innen. Anonymität werde demnach auch von deutschen Gerichten gestärkt.

Mod. AK: [Aufruf des letzten Redebeitrages]

Hörer_in: Greife das Grundrechtskonzept nicht mehr müsse der Staat hinterfragt werden. Problematisch sei die Ausweitung juristischer Ebenen durch den Konsum internationaler Dienstleistungen und der sich daraus ergebenden Konsequenzen für den Verbraucherschutz auf internationaler Ebene.

Mod. AK und RH: Abschluss der Diskussion, Dank für den vielfältigen Informationsaustausch. Verweis auf die Praxisveranstaltungen[41] der Veranstaltungsreihe zur Vermittlung von alltagstauglichen Handlungsoptionen gegen Überwachung. Verweis auf den Gastredner der folgenden Theorieveranstaltung II[42], Prof. Dr. Ernst-Günter Giessmann, und dessen Expertise nicht nur in kryptographischen Fragen, sondern auch hinsichtlich dessen praktischer Erfahrungen in der Mitentwicklung alltäglich eingesetzter Chipkartentechnologie. Bitte um Werbung und Kritik per E-Mail. Unter Applaus der Hörer_innenschaft Danksagung an die Gastredner_innen. Dank an die Hörer_innenschaft für die kompetente Diskussion. Verabschiedung.

41 http://jahr1nachsnowden.de/veranstaltungen (zuletzt aufgerufen: 02. Okt. 2015).

42 http://jahr1nachsnowden.de/veranstaltungen/th2 (zuletzt aufgerufen: 02. Okt. 2015).

Studentische Initiative:
„Edward - der Whistleblower, der nichts enthüllt hat?
Zum Vorwurf des "Digitalen Analphabetismus" im Jahr 1 nach Snowden“
Theorieveranstaltung II – „Vom Sinn der Kryptographie“ (01. Dez. 2014 – WiSe 2014/15)

Protokoll zur Veranstaltung „Vom Sinn der Kryptographie“

Gastredner_innen:	Leena Simon (LS)
	Prof. Dr. Ernst-Günter Giessmann (EGG)
Eröffnung, Moderation und Protokoll:	Roland Hummel (RH)

Initiatoren:	Amon Kaufmann (kaufmann@physik.hu-berlin.de)
	Roland Hummel (roland.hummel@theologie.hu-berlin.de)

Eröffnung

Aus gesundheitlichen Gründen könne der Mit-Initiator der stud. Initiative, Amon Kaufmann, an der aktuellen Veranstaltung nicht teilnehmen.

Die vorangegangene Veranstaltung „Vom Sinn des Privaten“ habe den Versuch unternommen, unter philosophischer Perspektive, aber auch durch Erkenntnisse aus dem Verbraucherschutz, das Konzept des Privaten im Zusammenhang mit der globalen Überwachungsaffäre zu untersuchen. Die philosophiegeschichtlichen Exkurse hätten, bspw. über Konzepte wie das des Panopticons aus dem 18. Jh., Überwachung als eine gesellschaftliche Problematik mit historischer Kontinuität verdeutlicht. Darüber hinaus sei für die Gegenwart durch die Erweiterung des zwischenmenschlichen Zusammenlebens in einen virtuellen Raum hinein die Notwendigkeit deutlich geworden, das Verhältnis von „privat“ und „öffentlich“ neu zu verhandeln.

Exkurs: „Saad Allami“

Ein zentrales Thema der letzten offenen Diskussion sei die Frage nach der persönlichen Betroffenheit durch globale Überwachung (Folie 2)[43] gewesen. Ein Beispiel für individuelle Betroffenheit durch Überwachung sei der Fall des Kanadiers Saad Allami aus dem Jahr 2012 (Folie 3), der sich wie folgt ereignet habe (Folie 4):

„Den 24. Januar 2012 wird Saad Allami aus dem kanadischen Quebec nicht so schnell vergessen. Als er gerade seinen siebenjährigen Sohn aus der Schule abholen wollte, fingen ihn Polizeibeamte ab und setzten ihn fest. Anschließend stürmten Ermittler seine Wohnung, durchkämmten die Räume und erklärten seiner Frau, sie sei mit einem Terroristen verheiratet. Arbeitskollegen von ihm wurden parallel dazu während einer Geschäftsreise in die USA an der Grenze abgefangen und mehrere Stunden zu ihren Verbindungen zu Allami befragt. Was war geschehen?

Saad Allami ist Vertriebsmanager bei einem Telekommunikationsunternehmen – und er ist unbescholtener kanadischer Bürger marokkanischer Abstammung. Drei Tage vor der Festnahme wollte er seine Kollegen motivieren, die sich gerade auf dem Weg zu einer Verkaufsmesse in New York City machten. Allami sendete ihnen eine SMS hinterher, sie mögen mit ihrer Präsentation die Konkurrenz „wegblasen“. Die kanadische Polizei durchleuchtete den Manager erst nach der Festnahme

43 Angaben der Folien dieses Abschnitts s. Anhang 4 »„Vom Sinn des Kryptographie“ – Präsentationsfolien der Eröffnung«.

gewissenhaft und stellte fest, dass der Terrorverdacht haltlos ist. Allami nutzte in seiner SMS das französische Wort „exploser“. Die Echtzeit-Analyse des US-amerikanischen Auslandsgeheimdiensts konstruierte offensichtlich aus der marokkanischen Herkunft, der abgefangenen SMS mit dem Begriff „explodieren“ und einer Truppe Einreisender als Empfänger der Nachricht eine Terrorwarnung.“[44]

In Verbindung mit der Thematik der aktuellen Veranstaltung ergebe sich die Frage, ob der Einsatz von Kryptographie im Nachrichtenaustausch zwischen Allami und seinen Mitarbeiter_innen diesen „Zwischenfall der Rasterfahndung“ hätte verhindern können (Folie 5).

Zur Klärung dieser und weiterer Fragen um das Thema der Kryptographie habe die Initiative zwei Gastredner_innen eingeladen: Leena Simon aus Bielefeld und Prof. Dr. Ernst-Günter Giessmann aus Berlin.

Vorstellung der Gastredner_innen

Leena Simon sei graduierte Philosophin sowie Netzpolitologin und beschäftige sich mit digitaler Mündigkeit und Technikpaternalismus. Desweiteren sei sie Aktivistin für das Konzept Freier Software und aktiv bei Digitalcourage e.V. tätig, einem Verein, dessen Tätigkeitsfeld auch aus der ehemaligen Eigenbezeichnung deutlich werde: „Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs“. Sie verfasse außerdem vielfach Online-Beiträge auf www.leena.de und www.netzphilosophie.org.

Prof. Dr. Ernst-Günther Giessmann sei Mathematiker und beschäftige sich seit 1990 mit Kryptographie. Seit 1996 sei er bei der Deutschen Telekom hauptberuflich beschäftigt und dort an der Entwicklung von Chipkartenprojekten beteiligt, so auch am elektronischen Reisepass und dem elektronischen Personalausweis. Parallel zu dieser Tätigkeit halte er Vorlesungen am Institut für Informatik der Humboldt-Universität zu Berlin.

Gastvortrag von Leena Simon

Der „Sinn des Privaten“ aus der vorangegangenen Veranstaltung werde, so Leena Simon, auch in ihrem Vortrag eine Rolle spielen, da sie selbst ebenfalls aus dem philosophischen Fachbereich stamme. So bestehe ihr Hauptanliegen in der Thematik der digitalen Mündigkeit. Unter diesem Begriff verstehe sie das verantwortungsbewusste Dasein des Menschen im digitalen Raum.

1. Verschlüsselung im Kontext der Verantwortung

Verantwortung beziehe sich in diesem Kontext erstens auf die eigene Kommunikation, die sich gesellschaftlichen Umständen anpassen müsse, wie aus Beispielen des täglichen Lebens deutlich werde: Ein unangemessen lautes Telefonat im öffentlichen Personennahverkehr bspw. verdeutliche die Problematik unverantwortlicher Kommunikation, da die hier ausgetauschten Informationen eventuell nicht im Einvernehmen des oder der zweiten Gesprächspartner_in öffentlich würden. In solchen Augenblicken sei Kommunikation in Bezug auf das Mithören intimer Informationen durch Fahrgäste zu

44 BLEICH, H.; „Globaler Abhörwahn“, in: c't Magazin für Computertechnik 16/2013, 112, online abrufbar unter: http://www.heise.de/ct/ausgabe/2013-16-Wie-digitale-Kommunikation-belauscht-wird-2317919.html – Kurzlink: http://heise.de/-2317919 (zuletzt aufgerufen: 03. Sep. 2015).

hinterfragen. Verantwortungsbewusste Kommunikation im öffentlichen Raum gehe daher bereits unbewusst mit Verschlüsselung fernab eines technischen Horizontes einher.

Exkurs „Soziale Verschlüsselung“

Die Reflexion über eine angemessene Art und Weise der eigenen Kommunikation sei demnach eine Art sozialer Verschlüsselung. Dies werde in der Kommunikation zwischen Erwachsenen und kleinen Kindern sehr deutlich, die Begriffe, bspw. das für Kinder meist sehr Appetit erweckende Wort „Eis“ mit „E-i-s“ verschlüsselten, oder sich mit zunehmendem Alter und Wissensstand der Kinder Fremdsprachen bedienten, um auf diesem Wege einer verbal-sozialen Verschlüsselung Informationen auszutauschen, welche die Ohren der Kinder nicht erreichen sollten. Verschlüsselung sei daher in ihrem grundsätzlichen Konzept keinesfalls ein Novum täglichen Lebens, sondern im Gegenteil bereits ein fester Bestandteil desselben.

Entsprechend stünden Bürger_innen auch in der Kommunikation innerhalb eines digitalen Raumes in der Pflicht, ihre Kommunikation den Gegebenheiten anzupassen. Schwierig werde diese Anpassung unter dem Umstand, dass soziale Netzwerke oft ein trügerisches Konzept von Privatheit suggerierten, deren Folge es sei, dass bspw. eine als privat empfundene Äußerung in soz. Netzwerken in Wahrheit eine öffentliche sei. Die sehr wandlungsfähige Konzeption des Privaten in virtuellen Räumen zu erkennen und als „Fallen“ für die eigene Wahrnehmung bewusst zu machen gehöre daher zum Aufgabenbereich verantwortungsbewusster Bürger_innen.

Bedauerlicherweise sei Verschlüsselung bspw. der eigenen E-Mailkorrespondenz mittels kryptographischer Schlüssel vor allem geräteübergreifend oft nur mit einigen Hürden zu nehmen, da alle Empfangsgeräte entsprechend erst einzurichten seien. Solche Hürden seien für Anwender_innen frustrierend, jedoch unumgänglich, wolle man die eigene Verantwortung im Umgang mit bspw. per E-Mail anvertrauten Informationen ernst nehmen.

2. Der Wert eines Geheimnisses

Die Bedeutung der Möglichkeit, Geheimnissen einen Raum zu geben, werde auf verschiedenen Ebenen deutlich.

2.1 ...auf machttheoretischer Ebene

Aus machttheoretischer Perspektive werde ersichtlich, dass umfangreiche Informationen es ermöglichten, über Individuen Macht auszuüben. Bereits auf Beziehungsebene werde dies deutlich, da durch gegenseitige Kenntnis der jeweiligen charakterlichen Eigenheiten Beziehungspartner_innen in der Durchsetzung punktueller Interessen genau wüssten, wie diese wohl am effektivsten zu erwirken wären. Diese Form von tolerierter Manipulation innerhalb einer Beziehung sei in diesem Fall nichts Negatives, da sie, unter Wahrung einer Beziehung „auf Augenhöhe“, auf gegenseitigem Einverständnis beruhe. In der Kommunikation im Internet jedoch sei der entscheidende Aspekt einer Kommunikation auf ausgewogener Ebene bzgl. global agierender Unternehmen und Geheimdienste nicht gegeben, sodass der gegenseitige Informationsstand ausschließlich zu Gunsten von Unternehmen und Geheimdiensten hinsichtlich Art und Umfang der von Bürger_innen gesammelten Informationen sei. Bürger_innen wären

demnach zunehmend schutz- und orientierungslos Angriffen und Manipulationen von Unternehmen und Geheimdiensten ausgeliefert. Dies betreffe auch die bereits real gegebene Möglichkeit der Verhaltenssteuerung von Individuen und Gruppen, abstrahiere man das Beispiel der gegenseitigen Möglichkeit zur Beeinflussung auf Beziehungsebene auf die Ebene zwischen Unternehmen und Geheimdiensten auf der einen sowie Nutzer_innen auf der anderen Seite, in welcher der Aspekt der Gegenseitigkeit nicht vorhanden sei.

2.2 ...auf gesellschaftlicher Ebene

In der Entwicklung von Ideen sei es überaus wichtig, Gedanken einen vor allgemeinem Zugriff sicheren Raum zu bewahren. Nur in einem geschützten Raum könnten Gedanken heranreifen, an Substanz gewinnen und auf diesem Weg gesellschaftlich sinnvolle Beiträge liefern. Das Konzept des Geheimnisses sei demnach die Keimzelle gesellschaftlichen Einfallsreichtums, da in diesem geschützten Raum die Möglichkeit bestehe, auch völlig unausgereiften Gedanken eine Entwicklung zu ermöglichen, die ohne das schützende Konzept eines Geheimnisses durch frühzeitige öffentliche Kommentierung kaum eine Überlebenschance hätten.

2.3 ...für das Konzept der Freiheit

Die fehlende Möglichkeit, Geheimnisse zu haben, sei Ausdruck einer Unfreiheit. Das Beispiel des Panopticons aus der vergangenen Veranstaltung habe dies sicher eindrücklich verdeutlicht. Das Bewusstsein einer beständigen Überwachung des eigenen Handelns, die mit der potentiellen Möglichkeit einhergehe, bestimmte Konsequenzen nach sich zu ziehen, verursache eine Anpassung des eigenen Handelns an angenommene Regeln hin zu einer Fremdbestimmung. Deutlich werde ein solches Moment der Fremdbestimmung bspw. beim Autofahren, gerate man unerwartet in den Sichtbereich eines Polizeiautos, worauf sich mitunter ein Affektzustand einstelle, der die eigene Fahrweise in gründlichster Weise nach geforderten Normen ausrichte.

2.4 ...in politischer Dimension

Überwachung von politischen Amtsträgern mache diese erpressbar, da die Akribie moderner Überwachungstechniken es ermögliche, Fehler und Schwächen eines jeden Menschen herauszufinden und dem Zweck der Erpressung dienstbar zu machen. Da politische Bekenntnisse von Fehlern oft mit einem Amtsrücktritt der bekennenden Person einhergehe, könne Erpressung, wolle die überwachte Person bspw. ihren Rücktritt verhindern, indem sie auf bestimmte Forderungen eingehe, in der Politik weit reichende Folgen nach sich ziehen. Das Geheimnis sei daher auch in politischer Dimension von Bedeutung, da eine politische Karriere in besonderer Weise davon abhängig sei, Geheimnisse erfolgreich wahren zu können. Durch Überwachung des politischen Bereiches ergebe sich folglich eine potentielle Erpressbarkeit einer jeden politischen Persönlichkeit und damit die unrechtmäßige Beeinflussung der Politik insgesamt.

Die mutmaßliche Überwachung des Mobiltelefons der Bundeskanzlerin Angela Merkel werfe in diesem Zusammenhang die Frage auf, warum eine Persönlichkeit, welcher die gesellschaftliche Dimension von Überwachung besonders auch durch das eigene Leben in der ehemaligen Deutschen Demokratischen

Republik alles andere als unbekannt sein müsste, bisher auf politischer Ebene gegen die globale Überwachungsaffäre nichts unternommen habe. Es dränge sich die Frage auf, ob auch hier gegen die Bundeskanzlerin eventuell Erpressung vorliege, die ein aktives Eingreifen ihrerseits verhindere.

Die sich einschleichende gesellschaftliche Vorahnung der potentiell jederzeit möglichen Enthüllung des privaten Lebensbereiches schaffe die Basis für Verschwörungstheorien, durch welche sich wiederum ein Vertrauensverlust in die Politik und damit schließlich ein Demokratieverfall ergebe. Das brisante an dieser Entwicklung, an deren Ende die Demokratie gefährdet werde, sei der bedrohliche Umstand, dass sie unabhängig von der Frage nach dem Wahrheitsgehalt der beobachteten Ereignisse verlaufe. Verschwörungstheorien seien folglich ein Problem für die Demokratie, sie ergäben sich im hier behandelten Kontext jedoch erst durch den Umstand der Überwachung.

2.5 ...in psychologischer Dimension

Geheimnisse dienten der Identitätsbildung. Dies werde bspw. in der Pubertät deutlich, in der die sich in der Entwicklung befindliche Identität häufig von Geheimnissen vor den Eltern begleitet sei, wobei der Raum der Geheimnisse dazu diene, die Struktur der eigenen Identität der eigenen Persönlichkeit gegenüber auszuhandeln und greifbar zu machen. Das Geheimnis ermögliche so das Konzept von Freiheit, Selbstbestimmung und Mündigkeit für die eigene Persönlichkeit umzusetzen.

3. „Nichts zu verbergen“?

Die in Bezug auf die Überwachungsthematik häufig vernommene, gleichgültige Aussage *„ich habe nichts zu verbergen“* sei unverschämt und einfältig. Dies werde unter mehreren folgenden Betrachtungen dieser Aussage deutlich.

Die Aussage sei 1. *falsch*, da jeder Mensch etwas zu verbergen habe. Dies werde an banalsten Alltäglichkeiten deutlich, angefangen bei der Benutzung einer Toilette, die für gewöhnlich unter Ausschluss der Öffentlichkeit aufgesucht und hier mit Selbstverständlichkeit ein privater Raum beansprucht werde.

Die Aussage sei 2. *dumm*, da sie den Zusammenhang von Freiheit, Geheimnissen und Macht außer Acht lasse.

Die Aussage sei 3. *rückwärtsgewandt*, da sie die Möglichkeit nicht in Betracht ziehe, in der Zukunft etwas zu verbergen zu haben. Das Argument ignoriere unter diesem Aspekt den Umstand der Wandelbarkeit dessen, was aktuell gesellschaftlich akzeptabel sei. Die Problematik werde deutlicher, beobachte man Verhaltensweisen einer vorangegangenen Generation, die akzeptiert, heute aber verächtlich betrachtet würden. Demnach sei die Aussage, nichts zu verbergen zu haben, generalisierend nicht möglich.

Die Aussage sei 4. *geschichtsvergessend*, da sie die Folgen radikaler Regierungswechsel außer Acht lasse. Über die Bevölkerung gesammelte Informationen ergäben in den Händen von radikalen Regimen, dies zeige die deutsche Geschichte, ein erschreckendes Missbrauchspotential.

Die Aussage sei 5. *unverschämt*, da die Implikation, etwas zu verbergen sei gleichbedeutend damit, etwas Falsches getan zu haben, Mitmenschen massiv unter Druck setze. Darüber hinaus zerstöre man

auf diese Weise die Möglichkeit, etwas verbergen zu dürfen, ohne sich verdächtig zu machen.

Der Aussage sei 6. *einschränkend*, da sich Bürger_innen einer geforderten öffentlichen Norm unterwerfen müssten, um toleriert zu werden. Das Verbergen von privaten Dingen, die eventuell nicht der öffentlichen Norm entsprächen, würde die Toleranz entsprechend einschränken.

Der Aussage sei 7. *naiv*, da Vertreter_innen das Potential jener Informationen unterschätzten, die sich aus freigebig veröffentlichen Informationen zusammenstellen ließen. Ein Pressesprecher eines Internetunternehmens gab für das Experiment einer Profilerstellung aus im Internet frei verfügbaren Informationen der Redaktion eines Computermagazins zunächst die Erlaubnis, die von ihm im Internet verfügbaren Informationen in einem Artikel zu veröffentlichen. Das Ergebnis der Zusammenstellung seiner Daten habe den Pressesprecher jedoch bei Vorlage des druckfertigen Artikels dazu bewogen, die Erlaubnis zur Veröffentlichung zurückzuziehen.[45]

Die Aussage *verhindere* 8. *Widerstand*, da eine Einstellung, nichts zu verbergen zu haben, kaum dazu beitrage, undemokratische Eingriffe durch den Staat wahrzunehmen und dagegen vorzugehen.

Geheimnisse seien damit notwendige Bedingungen für Freiheit und Selbstbestimmung. Demnach müssten Geheimnisse geschützt werden.

3.1 Komplexitätshürden für Kryptographie

Diesbezüglich spiele Kryptographie eine wesentliche Rolle, da das Internet heute ein Art Lebensraum darstelle oder sich zumindest zum Kommunikationsmittelpunkt etabliert habe. Die Kommunikation müsse den Gegebenheiten der Überwachung entsprechend angepasst werden, was bedeute, mit Kommunikationspartner_innen öffentlich einsehbare, daher unverschlüsselte, Kommunikationswege zu verlassen und private Kanäle mittels Kryptographie einzusetzen.

Hinderlich sei das unzureichend ausgeprägte Vorstellungsvermögen von Nutzer_innen, welches sich, dies werde auch an Äußerungen der Bundeskanzlerin Angela Merkel ersichtlich, noch immer im analogen Zeitalter befinde.[46] Der Übertritt in ein digitales Zeitalter sei, dies sehe man am Verhalten der Piratenpartei, jedoch eine Angelegenheit, die oftmals mit Leichtsinn verbunden sei. Die Piratenpartei habe mehrmals Parteitagsabstimmungen als Online-Petitionen behandelt und entsprechend das Abstimmungsverhalten für mehrere Jahre exakt protokolliert. Folglich seien aus diesen Parteitagsabstimmungen namentliche Abstimmungen geworden, die mit der Wahrung von Privatsphäre nicht vereinbar seien. Dieses Beispiel verdeutliche, dass auch unter sehr internetaffinen Bürger_innen ein ungenügend angepasstes Kommunikationsverhalten begegne.

Die Komplexität von Verschlüsselung sei aktuell für den Einsatz unter Normalnutzer_innen ein massives Problem. Allerdings seien sich Softwareentwickler_innen zunehmend dieser Problematik bewusst und versuchten mittels Projekten wie pEp[47] Verschlüsselung einfacher zu gestalten.

---

45 LINDEMANN, M.; SCHNEIDER, J.: "Datenschutz-Fallrückzieher", in: c't Magazin für Computertechnik 01/2011, 108, online abrufbar unter: http://www.heise.de/ct/artikel/Datenschutz-Fallrueckzieher-1153312.html?view=print – Kurzlink: http://heise.de/-1153312 (zuletzt aufgerufen: 03. Sep. 2015).

46 Anm. d. Pr.: Vgl. BEUTH, P.: „Die Kanzlerin von Neuland“, zeit.de, 19. Jun. 2013, online abrufbar unter: http://www.zeit.de/digital/internet/2013-06/merkel-das-internet-ist-fuer-uns-alle-neuland – Kurzlink: http://kurzlink.de/jMQUxJjFC (zuletzt aufgerufen: 03. Sep. 2015).

4. Fazit

Offensichtlich hätten Politik, Wirtschaft, Geheimdienste und vielleicht auch der oder die private Stalker_in, Interesse, private Informationen über Bürger_innen zu sammeln und private Kommunikation abzufangen. Gesetze gegen diese Überwachungspraktiken sind ein Lösungsansatz dieser gesellschaftlichen Spannung. Darüber hinaus gäbe es aber immer Instanzen, die sich selbst an sinnvolle, durchdachte Gesetze nicht halten. Aus diesem Grund seien Bürger_innen gefordert, ihre Kommunikation auch in Eigeninitiative abzusichern.

Leena Simon übergab das Wort mit der Frage, wie Kommunikation durch Verschlüsselung genau abgesichert werden könne, an Prof. Dr. Ernst-Günter Giessmann.

Gastvortrag von Prof. Dr. Ernst-Günter Giessmann

1. Einführung

Ernst-Günter Giessmann äußerte zu Beginn seines Vortrags, es gäbe zu seinem Bedauern zu wenige Veranstaltungen, die aus verschiedenen Perspektiven die Bedeutung technischer Bereiche wie den der Kryptographie untersuchten. Sein Vortrag stehe unter der Zielsetzung der Förderung einer gemeinschaftlichen Diskussion. Die Bedeutung der Kryptographie könne sich nur unter diesem Horizont erweisen lassen.

Am Beispiel der recht simpel verschlüsselten Willkommensbotschaft der Veranstaltung [Anm. d. Pr.: „Ifsamjdi Xjmmlpnnfo“ der Eingangspräsentation[48] – „Herzlich Willkommen“ mittels Caesar-Verschlüsselung[49]] könnten verschiedene Herangehensweisen der Kryptographie verdeutlicht werden, verschlüsselte Informationen zu entschlüsseln. So sei es ein Standardverfahren, verschlüsselte Informationen zunächst auf eine bestimmte Entschlüsselungsmethode hin zu analysieren (bspw. mittels statistischer Analysen, um die Häufigkeit wahrscheinlich auftretender Buchstaben und Wörter mathematisch vorherzusagen). Kryptolog_innen wählten allerdings immer den einfachsten Weg für einen Entschlüsselungsangriff. So sei in diesem Fall eine Entschlüsselung von „Ifsamjdi Xjmmlpnnfo“ allein aus dem Kontext der Situation dieser Veranstaltung möglich, um auf Buchstabenverschiebung mittels Caesar-Verschlüsselung und schließlich auf „Herzlich Willkommen“ zu schließen.

Unter „Verschlüsselung“ sei das Verbergen von Informationen vor unberufenem Mitlesen zu verstehen und basiere darauf, die Informationen zwischen Absender_in und Empfänger_in durch ein gemeinsames Geheimnis zu schützen. Daneben sei die hinter Verschlüsselung stehende Technik für eine zweite, ebenso bedeutende kryptographische Funktion zuständig: das Signieren. Signieren diene der Authentisierung von übertragenen Informationen, also einem Verfahren, welches sicherstelle, dass eine übertragene Information auf dem Transportweg nicht manipuliert wurde. Verschlüsselung sei daher nur ein Teil dessen, was unter dem Aspekt einer sicheren Informationsübertragung nötig sei. Der

47 „pretty Easy privacy“ in Anlehnung an das diesem zugrundeliegende, in seiner Komplexität aber kritisierte Verschlüsselungsverfahren PGP (Pretty Good Privacy): http://pep-project.org/ (zuletzt aufgerufen: 02. Okt. 2015).

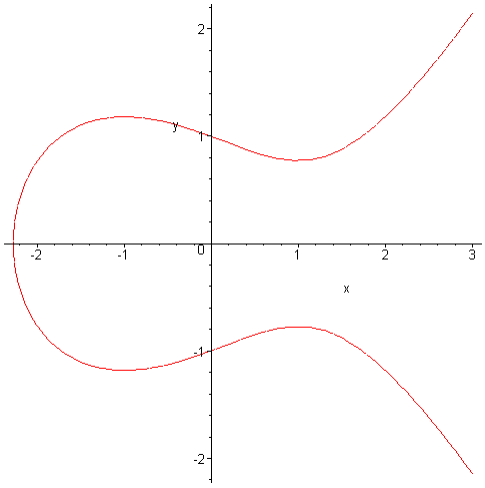
48 Folie 1 der Präsentation „Präsentation Einleitung RH“, online abrufbar im Bereich „Archiv“ unter http://jahr1nachsnowden.de/veranstaltungen/th2 (zuletzt aufgerufen: 02. Okt. 2015).

49 https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung (zuletzt aufgerufen: 02. Okt. 2015).

Umstand, dass eine E-Mail hochsicher verschlüsselt übertragenen wurde, beweise dem Empfänger nicht, dass ihr Inhalt auf dem Transportweg nicht doch manipuliert worden sein könnte. Schutz vor Überwachung und Manipulation biete daher nur die Kombination aus Verschlüsselung und Signierung, wobei die Signierung es dem Empfänger ermögliche, den entschlüsselten Datenbestand auf Manipulation hin zu prüfen (authentisieren). Der Zusammenhang von Verschlüsselung und Signierung in Bezug auf die Funktionen des dazu nötigen Schlüssels sei asymmetrisch zu verstehen: Verschlüsseln könnten alle (Nutzer_innen) für einen, Siegeln bzw. Unterschreiben könne einer für alle. Dieses Verfahren sei 1976 erstmals in einem kryptographischen Algorithmus umgesetzt worden. Die Besonderheit dieses asymmetrischen Verfahrens sei, dass das Ver- und Entschlüsseln von Computersystemen leicht durchgeführt werden könne und zugleich ein Rückschluss vom Verschlüsselungsalgorithmus auf den Entschlüsselungsalgorithmus (und umgekehrt) immens schwierig sei. In Bezug auf die Signierung bedeute dies, dass Signierung und Prüfung einer digitalen Unterschrift auf einem leicht durchführbaren Algorithmus basiere, der es zugleich jedoch immens schwierig mache, dadurch auf eine Möglichkeit schließen zu können, die Unterschrift zu fälschen.

2. „Wandern“ auf Elliptischen Kurven

Das Prinzip, einen mathematischen Berechnungsprozess leicht, seine Umkehrung allerdings immens schwierig zu gestalten, werde an einer elliptischen Kurve[50] deutlich:



Ausgehend von einem Punkt auf einer solchen Kurve ergebe sich ein zweiter Punkt, lege man an den ersten die Tangente an. Durch Wiederholung dieses Vorgangs mit jedem sich durch eine Tangente neu ergebenden Punkt „wandere“ man an der elliptischen Kurve entlang und es werde schon aus optischer Beobachtung deutlich, dass dieser Prozess der „Wanderung“ (an den sich immer neu ergebenden Punkten entlang) in eine Richtung sehr einfach vollzogen werden könne, der umgekehrte Weg jedoch (also eine Rückrechnung zum Ausgangspunkt) sehr schwierig sei. Dieses relativ moderne Verfahren namens „Rechnen auf einer elliptischen Kurve“ liege vielen aktuellen kryptographischen Verfahren zugrunde, bspw. der Verschlüsselung von Informationen im Reisepass, aber auch in der Verschlüsselung und Signierung von E-Mails.

Bemerkenswert sei der Umstand, dass bisher kein modernes kryptographisches Verfahren gebrochen wurde. Aus mathematischer Sicht seien gängige Verfahren durchweg extrem gut, Schwächen gäbe es aber durchaus immer wieder zum einen in der Umsetzung, also an der Infrastruktur der Software, zum anderen in der Anwendung des Verfahrens durch den Benutzer. Darüber hinaus gibt es bei jedem kryptographischen Algorithmus bestimmte Parameter, die zu einer Schwächung des Verfahrens führten.

50 Abb.: „Ell kurve“ von Fredstober - Mit Maple erzeugt: implicitplot(5*y^2 = x^3 - 3*x + 5,x=-3..3,y=-3..3, numpoints=1000);. Lizenziert unter PD-Schöpfungshöhe über Wikipedia – https://de.wikipedia.org/wiki/Datei:Ell_kurve.png#/media/File:Ell_kurve.png (zuletzt aufgerufen: 02. Okt. 2015).

3. Beispiele für gebrochene Verschlüsselungsverfahren

Der Verschlüsselungsklassiker ENIGMA aus dem Zweiten Weltkrieg sei technisch gebrochen worden, weil zum einen ihr technischer Aufbau untersucht werden konnte, zum anderen aber auch durch pragmatische Analysen: Wusste man bspw., dass es bei einem verschlüsselten Text kontextuell um die Übermittlung von Wetterinformationen ging, konnte man anhand von Vergleichen zwischen verschlüsseltem und unverschlüsseltem Text Schlussfolgerungen auf die verwendeten Chiffrier-Schlüssel ziehen, die zur Entschlüsselung stark beitrugen. Der MIFARE-Chip, ein Chip zur kontaktlosen Kommunikation, sei gebrochen worden, nachdem man ihn über Jahrzehnte ohne Rücksicht auf Fortschritte in der Kryptoanalyse unverändert verbaut habe.[51] Der Personalausweis bspw. sei zwar selbst nicht gebrochen worden, jedoch seine Infrastruktur durch die Verwendung ungenügend sicherer Chipkartenleser zum Auslesen der auf dem Ausweis gespeicherten Daten. Sicherheitslücken wie „Heartbleed“ und „Shellshock“ aus der jüngsten Vergangenheit seien ebenso auf menschliches Versagen in der hinreichenden Implementierung kryptographischer Verfahren zurückzuführen.

4. Verhältnis von Verschlüsselung zu anderen Sicherheitsparametern

In der Verwendung von Kryptographie im E-Mail-Verkehr werde deutlich, wie wichtig die Verwendung von starken Parametern in Form von sicheren Passwörtern sei, daneben jedoch auch, wie unbequem die Anwendung von Kryptographie werden könne, wenn eben diese Parameter zu stark (und die gewählten Passwörter entsprechend zu komplex) würden. Dadurch würden kryptographische Verfahren geradezu unbequem und anwenderunfreundlich. Aus der Perspektive des Marketings entstehe so ein Zwiespalt von Bequemlichkeit und Sicherheit. Aus kryptologischer Sicht bestehe diese Wahl jedoch eher zwischen Unsicherheit und Unbequemlichkeit.

Verschlüsseln ermögliche den Schutz vor unberufenem Mitlesen und werde dadurch ein Garant für Privatsphäre. Jedoch setze der sinnvolle Einsatz von Verschlüsselung voraus, dass auch Adressat_innen von verschlüsselten Informationen mit den ihnen anvertrauten Informationen den Schutz vor unberufenem Mitlesen auch nach dem Empfang zu gewährleisten wüssten. Verschlüsselung entfalte demnach nur dann die gewünschte Sicherheit, wenn sie einherginge mit dem Wissen um Anonymisierung der Korrespondent_innen (bspw. durch Pseudonyme), Integrität des Nachrichteninhalts, Authentizität des Absenders oder die Möglichkeit der plausiblen Abstreitbarkeit einer stattgefundenen Kommunikation.[52]

Die Möglichkeit, das Internet als Kommunikationsmedium zu nutzen, gehe mit der Verwendung von Standards einher, an die sich Kommunikationspartner_innen für eine universelle Kommunikation halten müssten, wollten sie entsprechend universell erreichbar sein. Dies ziehe zwangsläufig nach sich, dass der Einfluss auf bestimmte (der sicheren Kommunikation eventuell nicht zuträgliche) Parameter den Nutzer_innen zwangsläufig entzogen wären. Ein solcher Einfluss sei nur durch die Verwendung eigener Kommunikationsverfahren gewährt, die den gewünschten Kommunikationspartner_innen dann zuerst

51 https://de.wikipedia.org/wiki/Mifare (zuletzt aufgerufen: 02. Okt. 2015).

52 https://de.wikipedia.org/wiki/Glaubhafte_Abstreitbarkeit (zuletzt aufgerufen: 02. Okt. 2015).

mit der einhergehenden Umständlichkeit vermittelt werden müssten. Die Vielfalt und Leistungsfähigkeit aktueller technischer Geräte ermögliche den niedrigschwelligen Einsatz kryptographischer Verfahren, zum Beispiel das Rechnen auf elliptischen Kurven, für jedermann, sofern diese Verfahren unter standardisierten Umgebungen erfolgten.

Die Personalausweis- und Reisepassinfrastruktur eines jeden Landes ermögliche die Authentisierung des jeweiligen Passes. Der Vatikan verwende in seiner Infrastruktur kryptographische Schlüssellängen von 4096 Bit, was ein vergleichsweise sehr hohes Sicherheitsniveau ermögliche. Ein weiterer Parameter der vatikanischen Passinfrastruktur verwende jedoch einen Wert, der bereits seit ca. 20 Jahren als unsicher einzustufen sei.[53] Aus diesem Beispiel solle deutlich werden, dass bspw. die Verwendung großer Schlüssel kein Garant für eine sichere Infrastruktur sei, wenn weitere wichtige Parameter nicht auf adäquatem Level gewählt würden.

5. Verschlüsselung im interdisziplinären Diskurs

Eine rein technische Lösung für den Schutz der Privatsphäre sei nicht zu realisieren. Interdisziplinäre Veranstaltungsreihen böten die Voraussetzung dafür, den Dialog zwischen technischen und philosophischen Fachbereichen sowie der Nutzer_innenschaft zu eröffnen und der Komplexität zum Schutz der Privatsphäre zu begegnen.

6. Erinnerung an Carl von Ossietzky

Die Veranstaltungsreihe „Jahr 1 nach Snowden“ weise schon in ihrem Titel auf die Bedeutung von Menschen hin, die auf untragbare gesellschaftliche Zustände hinwiesen und Diskurse wie den aktuellen über die Privatsphäre erst ermöglichten. Dem deutschen Journalisten Carl von Ossietzky sei im Zusammenhang der herausragenden gesellschaftlichen Bedeutung von Whistleblowern an dieser Stelle eine besondere Würdigung zukommen zu lassen. Unter einem Pseudonym wurde im Mrz. 1929 in der Zeitschrift „Die Weltbühne“, deren Herausgeber Ossietzky war, unter dem Titel „Windiges aus der deutschen Luftfahrt“ die verdeckte Aufrüstung der deutschen Luftwaffe enthüllt. Carl von Ossietzky wurde daraufhin aufgrund des Verrates militärischer Geheimnisse verurteilt. Ossietzky erhielt im Jahr 1936 rückwirkend den Friedensnobelpreis für das Jahr 1935. Diese Ehrung komme in den nächsten Tagen eine weitreichende Bedeutung zu, da die Internationale Liga für Menschenrechte im einhundertsten Jahr ihres Bestehens am 14. Dez. 2014 die Carl-von-Ossietzky-Medaille an die, durch die globale Überwachungsaffäre eng miteinander verbundenen, Persönlichkeiten Glenn Greenwald, Laura Poitras und Edward Snowden verleihen werde.[54]

Mit der Bitte um Spenden für die wichtige Arbeit der Internationalen Liga für Menschenrechte schloss Prof. Dr. Giessmann seinen Vortrag.

---

53 Dies betreffe laut Prof. Dr. Giessmann den öffentlichen Exponenten des RSA-Verfahrens, der im Fall des Vatikans „3“ betrage und damit ein unsicheres Niveau habe.

54 Pressemitteilung der Internationalen Liga für Menschenrechte vom 15. Nov. 2014: „Festakt zur Verleihung der Carl-von-Ossietzky-Medaille 2014 an Edward Snowden, Laura Poitras und Glenn Greenwald am 14. Dezember 2014, um 11:00 Uhr in der Urania Berlin“, online abrufbar unter: ilmr.de/2014/festakt-zur-verleihung-der-carl-von-ossietzky-medaille-2014-an-edward-snowden-laura-poitras-und-glenn-greenwald-am-14-dezember-2014-um-1100-uhr-in-der-urania-berlin – Kurzlink: http://kurzlink.de/AvD7Mkjbv (zuletzt aufgerufen: 02. Okt. 2015).

Offene Diskussion der Gastvorträge

Abkürzungen der Namen:
LS: Leena Simon
EGG: Prof. Dr. Ernst-Günter Giessmann
Mod. RH: Roland Hummel (Moderation)

Nach einer fünfminütigen Pause erfolgte unter der Moderation von Roland Hummel die offene Diskussion der Gastvorträge.

Hörer_in: [an LS] Es hieß, Verschlüsselung von Kommunikation müsse zentrales Anliegen seitens der Bürger_innen sein, um auf die Überwachungsaffäre angemessen zu reagieren. Daneben stelle sich jedoch die Frage, ob ein solcher gesellschaftlicher Druck zur Verschlüsselung diese nicht in ihrer Freiheit einschränke und dem Grundsatz entgegenstehe, in einer freien Gesellschaft auf den Schutz durch diese vertrauen zu können. Obgleich der Staat aktuell diesem Schutz nicht nachkomme, stelle sich dennoch die Frage, ob die Argumentation, sich den gesellschaftlichen Gegebenheiten durch Verschlüsselung anzupassen, nicht die Möglichkeit vernachlässige, die gesellschaftlichen Gegebenheiten grundlegend zu ändern, sodass Bürger_innen wieder auf den Schutz des Staates vertrauen könnten.

LS: [an Vorredner_in] Selbstverständlich sei Selbstschutz durch Verschlüsselung nur eine Maßnahme neben anderen, wichtigen gesellschaftlichen Bestrebungen, die gesellschaftspolitischen Gegebenheiten durch nationale wie europäische Proteste zu ändern und durch Informationsveranstaltungen Bürger_innen an ihre Verantwortung der gesellschaftspolitischen Mitgestaltung zu erinnern. Der „technologische Arm“, in diesem Fall der der Kryptographie, sei nur einer von vielen. Zu diesem Zweck empfinde es LS als durchaus angemessen, neben Portalen wie Twitter auch Facebook zu nutzen, um Bürger_innen zu erreichen, auch wenn diese stets in der Kritik von datenschutzsensiblen Vereinen wie digitalcourage stünden. Die Arbeit im Internet für mehr Datenschutzbewusstsein sei nur auf breiter Front effektiv, sodass neben freien Portalen wie (ehemals) identi.ca mit gewissen Bedingungen auch Facebook einzusetzen sei, bspw. mit der Direktive, immer nur aus Facebook heraus zu verweisen, nie jedoch in Facebook hinein. Intensive Diskussionen seien der Schlüssel, ein entsprechendes Bewusstsein darüber zu schaffen, wie mit dem eigenen öffentlichen und privaten Raum sowie dem Umgang der eigenen Daten in Bezug auf diese angemessen umzugehen sei.

Hörer_in: Das durchaus schlüssige Argument von Staaten, ihre Bürger_innen durch Überwachungssysteme vor gewalttätigen Übergriffen schützen zu wollen, stehe im Konflikt mit der Forderung nach allumfassender Verschlüsselung von Informationen und dieser Konflikt zwischen negativen Folgen von Überwachung und Schutz durch Überwachung lasse sich persönlich schwer zufriedenstellend auflösen. Daher gehe die Frage an LS und EGG, ob Konzepte zum Umgang mit diesem Dilemma existierten.

LS: [an Vorredner_in] Einhundertprozentige Sicherheit könne es weder in der virtuellen noch in der analogen Welt geben. Die Frage müsse daher in Bezug auf ihre Verhältnismäßigkeit und in der Abwägung der jeweiligen Gefahren besprochen werden. Die eigentliche Gefahr bestehe in der Abschaffung von demokratischen Grundstrukturen durch Überwachung, da diese durch eine

allumfassende Drohkulisse permanenter Überwachung das Bewusstsein der Bürger_innen massiv beeinträchtige, im Angesicht gesellschaftspolitischer Missstände gefahrlos ihr Mitbestimmungsrecht wahrnehmen zu können. Die Gefahr für die Auflösung demokratischer Mechanismen sei aktuell sehr viel akuter als diejenige der Bedrohung durch terroristische Übergriffe. Absicherung sei dabei durch Demokratie gewährleistet, nicht durch Überwachung.

Hörer_in: [an Vorredner_in] Persönlich sei eine solche Sichtweise nachvollziehbar, allerdings müsse die Gesellschaft dann auch terroristische Übergriffe akzeptieren.

LS: [an Vorredner_in] In gleichem Maße würden Autounfälle akzeptiert werden, ohne deswegen den Straßenverkehr gänzlich abzuschaffen.

Hörer_in: [an EGG] Rückfrage, wie die im Vortrag erwähnte Methode des „digitalen Versteckens“ möglich sei und, ob diese etwas mit dem Löschen von Daten zu tun habe.

EGG: [an Vorredner_in] Die Möglichkeit eines simplen Löschvorgangs digitaler Informationen sei ein Missverständnis. Digitale Informationen wie „47/11“ oder die Zahl „2“ könnten nicht ohne weiteres eliminiert werden, da digitale Informationen im Allgemeinen keinen Träger hätten, auf dem sie sich befinden. Durchaus sei es natürlich möglich, Datenträger zu löschen, auf denen sich eine Information befindet, aber nicht die Information selbst. Dieser Sachverhalt verdeutliche, was hinter der Redewendung „Das Internet vergisst nichts!“ stehe. Das Verstecken von Daten sei hingegen möglich, indem Informationspakete genutzt würden, die sehr viel „Unschärfe“ enthielten. bspw. könne man in dem Informationspaket eines digitalen Fotos, welches durch die Technik heutiger Digitalkameras eine riesige Menge an Daten enthalte, an eine Information wie einen Text verstecken, ohne, dass dies später im Bild optisch ersichtlich sei.[55] Adressat_innen eines Kommunikationsvorgangs könnten dadurch indirekt verborgen werden, dass bspw. eine an sie gerichtete E-Mail eine einzelne in einer Unmenge von verschlüsselten E-Mails mit unterschiedlichen Adressat_innen sei, von denen die Masse aber inhaltlich keinerlei Bedeutung habe, also „Datenmüll“ sei und die inhaltlich bedeutsame E-Mail verschleiere.

Hörer_in: [an Vorredner_in] Die zuletzt beschriebene Methode bedeute einen Aufwand, der für den Alltag nicht praktikabel sei. Grundlegend ergebe sich die Frage, warum Bürger_innen für die Gewährleistung von Grundrechten die „Bringschuld“ obliege. Dies bedeute für Nutzer_innen digitaler Dienste in der Regel eine massive Überforderung, sich in die nötigen Verfahren zur Gewährleistung des Datenschutzes intensiv einarbeiten zu müssen.

EGG: [an Vorredner_in] Diese Problematik bestehe durchaus, es sei lediglich auf die Frage eingegangen worden, wie es theoretisch möglich sei, digitale Informationen zu verstecken. Die Möglichkeit, das Ereignis einer Kommunikation nachträglich abstreiten zu können, sei daneben eine besondere Problematik.

Hörer_in: Es ergebe sich die Frage, was von neuen Kommunikationsmitteln wie der „De-Mail“[56] in diesem Zusammenhang an Sicherheit vor Überwachung oder Spionage zu erwarten sei.

55 Anm. d. Mod.: Vgl. https://de.wikipedia.org/wiki/Steganographie (zuletzt aufgerufen: 02. Okt. 2015).

56 https://de.wikipedia.org/wiki/De-Mail (zuletzt aufgerufen: 02. Okt. 2015).

EGG: [an Vorredner_in] Für den Privatgebrauch sei der Schutz, den das angesprochene Verfahren biete, nicht ausreichend. Der „De-Mail“-Dienst könne mit Briefen per Einschreiben verglichen werden, wodurch sich ein Nachweis über die digitale Zustellung der De-Mail ergebe und ihr Schutz auf dem Kommunikationsweg gewährleistet sei. Für den behördlichen Schriftwechsel bedeute dies aber durchaus einen Mehrwert.

LS: [an Vorredner_in] An Projekten dieser Art bestehe vor allem durch die Vermutung Kritik, sie besäßen eingebaute Hintertüren, wodurch sich die Problematik „defective by design“ [„fehlerbehaftet ab Werk“] ergebe.

EGG: [Einspruch an Vorredner_in] Die Aussage könne nicht als gänzlich richtig bestätigt werden. Am Beispiel des Briefes per Einschreiben würde aber das problematische Verfahren der De-Mail deutlich werden. Werde ein solcher Brief bspw. bei Postdienstleister A abgegeben, erfolge die Zustellung im Falle der De-Mail nicht ebenfalls durch Postdienstleister A, sondern durch eine Kette weiterer Postdienstleister. Bei jedem Wechsel des Postdienstleisters werde der Umschlag geöffnet und der Brief in einen neuen gesteckt. Dieses Verfahren könne durchaus als fehlerhaft in der Konzeption angesehen werden. Vertraue man allerdings den Postdienstleistern von vorneherein nicht, ergebe sich auch kein Vorteil für die Sicherheit, würde die Nachricht nur von einem einzelnen Postdienstleister zugestellt werden. Der Aspekt eines kontrollierten Transportweges könne neben der rechtsgültigen Zustellbestätigung durchaus als Mehrwert betrachtet werden.

Hörer_in: Dem Einwand, Verschlüsselungsverfahren seien in ihrer Anwendbarkeit für Nutzer_innen zu kompliziert, müsse stattgegeben werden. Aus der Sicht der Softwareentwicklung [Hörer_in zählt sich in diesen Berufszweig] zeige der aktuelle Stand der Softwaretechnik zwar sichere, aber schlecht benutzbare Systeme. Das angesprochene Verfahren zum Verstecken von Informationen sollte eigentlich durch Softwaretechnik automatisch durchgeführt werden, ohne manuelles Eingreifen der Nutzer_innen. Dies sei vom Designprozess her durchaus möglich. Etablierte Software habe diese Problematik auch im Blick, wie bspw. an der vor kurzem eingeführten Verschlüsselung in der Smartphoneapplikation WhatsApp deutlich werde. Große IT-Konzerne nähmen Bemühungen auf sich, ihre Produkte sicherheitstechnisch zu verbessern.

Hörer_in: [an EGG] Der Aussage, die De-Mail sei für den privaten Gebrauch nicht empfehlenswert, für den öffentlich-behördlichen Bereich jedoch durchaus, müsse widersprochen werden. Unter Berücksichtigung der Tatsache, dass Anwält_innen höchst sensible Daten zu verarbeiten hätten, sei das beschriebene Verfahren der De-Mail, durch welches jeder Postdienstleister den virtuellen Umschlag auf dem Transportweg öffnen müsse, fatal. Einzig Ende-zu-Ende-Verschlüsslung, welche Verschlüsslung und Signierung durch die Absender_innen selbst ermögliche, sei ein wirksames Verfahren, vertrauliche Informationen sicher zu übermitteln.

EGG: [an Vorredner_in] Grundsätzlich sei der Aussage zuzustimmen, jedoch sei der aktuelle Stand in Behörden, so auch Gerichten, auf einem Niveau, der bereits den Empfang von lediglich signierten E-Mails schon nicht erlaube.

Hörer_in: [an EGG] Zumindest werde diesem Problem durch ein relativ neues Gesetz begegnet, welches ab 2022 die verschlüsselten Korrespondenz für den juristischen Bereich vorschreibe.[57]

Hörer_in: Der Ruf von Nutzer_innen nach leicht anwendbaren Verschlüsselungsverfahren in Software gehe oft in Richtung Freier Software[58]. Gleichzeitig seien Nutzer_innen oftmals nicht bereit, die Programmierer_innen für ihre Arbeit zu bezahlen, da die Bereitstellung Freier Software zunächst in der Regel kostenlos erfolge. Sicherheit durch transparent programmierte Software sei jedoch nur dann nachhaltig möglich, wenn Endanwender_innen ihre Einstellung in Bezug auf die Entlohnung der Programmierer_innen änderten oder bereit seien, für Software zu bezahlen.

LS: [an Vorredner_in] Der Begriff „frei“ werde oft im monetären Sinn verstanden und dabei „kostenlos“ mit „kostenfrei“ verwechselt. Freie Software habe zunächst mit „kostenlos“ nichts zu tun und könne durchaus kommerziell verkauft werden. Die vielfach zu beobachtende Einstellung, einen Service ohne finanzielle Gegenleistung nutzen zu wollen, beruhe auf dem Missverständnis, auch in der Nutzung eines finanziell kostenlosen Produktes einen Kund_innen-Status inne zu haben. Es sei jedoch viel eher davon auszugehen, dass die Nutzung kostenloser Services die Nutzer_innen vielmehr zum Produkt machten. Die Einsicht, für eine Serviceleistung zu zahlen, gewährleiste den eigenen Status eines „Kunden“ statt eines „Produktes“. Unabhängig davon bestehe der Wert von Freier Software vor allem in der Möglichkeit, den Quellcode nachvollziehen zu können. Dies sei auch für Programmierunkundige von Bedeutung, vergleichbar mit dem Umstand, die die eigene Person betreffenden Landesgesetze prinzipiell nachvollziehen zu können, auch wenn dafür in der Regel Jurist_innen zu Rate gezogen werden müssten, da Gesetzestexte in der Regel für Laien ebenso unverständlich seien wie ein Programmcode. Durch Freie Software sei anders als bei proprietärer Software das Recht gegeben, Quellcode nachvollziehen zu können und dies sei ebenso wichtig wie die prinzipielle Nachvollziehbarkeit von Gesetzestexten, die ebenso einen Einfluss auf das eigene Leben hätten wie Software im digitalen Zeitalter. Um eine solche Transparenz gehe es dem Freiheitsbegriff in Freier Software. Die aktuell noch freiheitliche Gesellschaftsordnung werde aus Desinteresse aufgegeben. Das Desinteresse an sich etablierenden totalitären gesellschaftlichen Strukturen sei vergleichbar mit dem Desinteresse, für einen Service oder eine Software Geld zu zahlen, welches wiederum Ausdruck einer Bequemlichkeitshaltung sei, die erstens alles für eine kostenlose Smartphone-Applikation opfere, was vorangegangene Generationen gesellschaftlich hart erkämpft hätten, und zweitens sich so der Verantwortung zum Erhalt schwer erkämpfter Freiheitsrechte entziehe.

Hörer_in: [an Vorredner_in] Die Vermutung liege nahe, dass sichere und einfach zu bedienende Software aktuell deswegen nicht existieren, weil die Nutzer_innenschaft sich aktuell in einer Anspruchshaltung befinde, unter der eine Finanzierung der gewünschten Software, nämlich frei, kostenlos und sicher, nicht möglich sei.

Mod. RH: Die folgenden Fragen müssten aus zeitlichen Gründen gebündelt erfolgen.

---

57 „Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten“ vom 10. Okt. 2013: http://dipbt.bundestag.de/extrakt/ba/WP17/500/50035.html – Kurzlink: http://kurzlink.de/PcB5v5StG (zuletzt aufgerufen: 02. Okt. 2015).

58 https://de.wikipedia.org/wiki/Freie_Software (zuletzt aufgerufen: 02. Okt. 2015).

Hörer_in: [an Vorredner_in] Es sei ein merkwürdiger Gedanke, bereits bestehende Grundrechte durch zusätzlichen finanziellen Einsatz der Nutzer_innen (in sichere Software) geschützt werden müssten. Es sei nachvollziehbar, dass ehrenamtliche Entwickler_innen für ihre Arbeit entlohnt werden sollten. Dieses Problem bestehe allerdings unabhängig von der aktuellen Situation des massiven Verstoßes gegen Grundrechte in der Überwachungsaffäre und es sei schwer nachvollziehbar, warum Bürger_innen nun dafür zahlen sollten, um dieses Grundrecht zu erhalten oder überhaupt einzufordern. Es könne nicht sein, dass jemand, der aus welchen Gründen auch immer, kein Geld für sichere Software ausgeben kann, der Überwachung schutzlos ausgeliefert sei.

Hörer_in: Aus Sicht weniger technikversierter Nutzer_innen erscheine die Möglichkeit von Geheimdiensten und Konzernen unwirklich, die immensen Datenmengen zum Nachteil der Nutzer_innen aufbereiten zu können. Daher sei das Problem aufwendiger Verschlüsselungsverfahren ein zweitrangiges vor der Vermittlung der Möglichkeiten, die jene Datenmengen ermöglichten, die Bürger_innen durch kostenlose Programme preisgäben.[59]

Hörer_in: Die Schuldzuweisung gegenüber Normalverbraucher_innen, die sich nach und nach dem Stand der Technik zu Nutze machten und entsprechend Smartphones und soziale Netzwerke ohne größeres technisches Hintergrundwissen nutzten, sei unangebracht. Es gelte nun, die angesprochenen Probleme wie der Unterfinanzierung von Freier Software sowie dem mangelnden Datenschutzbewusstsein der Bevölkerung mit politischen Lösungen zu begegnen.

LS: [an Vorredner_innen] Auch für einen Brief, den man verschickt, sei es selbstverständlich, Geld zu bezahlen. Bei der Nutzung eines kostenlosen E-Mail-Services werde jedoch in der Regel ungelesenen AGB zugestimmt, die das Grundrecht einer überwachungsfreien Nachrichtenübermittlung aushebelten. Das zentrale Problem bestehe in der Priorisierung der Bürger_innen von kostenlosen Services gegenüber der Integrität ihrer Grundrechte. Es sei rückwirkend schwer deutlich zu machen, für einen Service selbstverständlich zu bezahlen, damit Grundrechte gewahrt blieben, da nunmehr, nachdem sich ein solcher Habitus einmal etabliert habe, nach kostenlosen Services verlangt werde, die dennoch die Grundrechte wahrten und nicht gesehen werde, dass die Bedingung für den kostenlosen Service die Aushebelung von Grundrechten sei. Ebenso verschicke die Post keine Briefe ohne Briefmarke. Politisch müsse hier selbstverständlich ebenfalls gewirkt werden und bspw. statt der Investition in elektronische Gesundheitskarten dezentrale IT-Infrastrukturen gefördert werden. Freiheit stehe jedoch aber immer zugleich in der Verantwortung der Bürger_innen. Das Individuum könne sich nicht in der Masse und hinter der Forderung nach Lösungen von Problemen durch die Gesellschaft verstecken. In erster Linie sei das Individuum für die eigene Mündigkeit und Selbstbestimmung permanent selbst verantwortlich. Dies begründe sich in dem Umstand, dass mit Rechten, so auch den Grundrechten, gewisse Pflichten einhergingen, von denen eine wichtige sei, die Grundrechte zu verteidigen – vor allem in Angesicht von kostenlosen Services. Hier müsse dem Individuum deutlich werden, dass es zwar für Freie Software nicht bezahlen müsse, aber die Freiheit habe, für einen vielfach genutzten Lieblings-Service im Internet

59 Anm. d. Pr.: Vgl. WOLFIE, C.: „Kommerzielle digitale Überwachung im Alltag“, Studie von Cracked Labs im Auftrag der österreichischen Bundesarbeitskammer, 2014, online abrufbar unter: http://crackedlabs.org/studie-kommerzielle-ueberwachung/info (zuletzt aufgerufen: 02. Okt. 2015).

spenden zu können. Es sei eine bequeme Position, die Verantwortung auf andere abzuschieben, so wie es durchaus auch die Bundesregierung mit der Aufforderung tat, Bürger_innen müssten für ihre Sicherheit im Internet selbst Sorge tragen.[60] Staat und Bürger_innen stünden gleichermaßen für den Schutz der Grundrechte in der Verantwortung.

EGG: [an Vorredner_innen] Der Wunsch nach gewährleistetem Schutz auch bei kostenlosen Services sei nachvollziehbar, aber die ungeschützte Nutzung des Internets sei kein Vorgang, bei dem ein Service genutzt werde, sondern durch den Nutzer_innen selbst zu Produkten gemacht würden. Es müsse deutlich werden, dass in der Nutzung des Internets die Datenprofile von Nutzer_innen beständig geerntet würden.

Hörer_in: Neben der Möglichkeit, Informationen zu verstecken, sei eine weitere wichtige Methode, in der Übermittlung von Informationen im Internet stets den kürzesten Weg zu bevorzugen. Ein Nachrichtenaustausch innerhalb von Europa müsse nicht über nordamerikanische Netzknotenpunkte laufen.

EGG: [an Vorredner_in] Das Internet sei ursprünglich gerade nicht daraufhin konzipiert worden, in der Übermittlung von Daten stets den kürzesten Weg zu wählen, sondern daraufhin, Wege zu wählen, die der sicheren Informationsübermittlung Priorität in der Wahl des Informationsweges gebe. Dennoch sei es technisch kein Problem, die Informationswege so zu gestalten, dass sie, sollten sich Absender_in und Empfänger_in in den selben nationalen Grenzen aufhalten, in diesen blieben. In Bezug auf die Überwachung durch „dreibuchstabige Organisationen“ sei das Problem aber nicht in Übersee zu verorten, sondern beginne bereits in den eigenen nationalen Grenzen, bspw. an wichtigen Knotenpunkten wie Frankfurt am Main.

Hörer_in: [an EGG] Die Frage sei, warum Informationen über Frankfurt (Main) geleitet werden müssten, sollten sich Absender_in und Adressat_in bspw. in Berlin aufhalten. Der Umstand, dass das Internet nicht von allein den kürzesten Weg wähle, sei der historisch-technischen Entwicklung geschuldet und müsse an die gegebenen Zeitumstände angepasst werden, obgleich es hohen technischen Aufwand erfordere. Dahinter stehe nicht der Versuch, Informationen abzuschotten oder Länder auszuklammern, sondern durch effiziente Übermittlung die Möglichkeiten zur Überwachung zu minimieren.

LS: [an Vorredner_in] Das Probleme bestehe bereits in der unkomplizierten Dateiübertragung zwischen Geräten des eigenen Heimnetzwerkes. Diese sei faktisch nicht gegeben, sodass man sich häufig dabei erwische, Dateien von einem Gerät zum anderen per E-Mail zu schicken, weil dies am unkompliziertesten sei.

Hörer_in: Der Umstand, dass Geheimdienste wie der BND Sicherheitslücken kauften, um auf Geräte von Nutzer_innen zugreifen zu können, stelle die Absicherung durch Kryptographie immens in Frage.[61]

60 Anm. d. Pr.: Vgl. „Nationalstaat beim Datenschutz überfordert“, Bayern 2 vom 16. Jul. 2013: http://www.br.de/presse/inhalt/pressemitteilungen/bayern2-radiowelt-176.html – Kurzlink: http://kurzlink.de/eDF7zgISb (zuletzt aufgerufen: 02. Okt. 2015).

61 Anm. d. Pr.: Vgl. „SSL abhören: Kritik an BND-Plänen zu Zero-Day-Exploits“, heise Security vom 10. Nov. 2014: http://www.heise.de/security/meldung/SSL-abhoeren-Kritik-an-BND-Plaenen-zu-Zero-Day-Exploits-2445246.html – http://kurzlink.de/4M0xPJ24B (zuletzt aufgerufen: 02. Okt. 2015).

Sichere Kommunikation sei zudem nicht möglich, weil auch innerhalb der Informatik klar sei, dass es niemals völlig sichere Programme geben könne.

Hörer_in: Viele der angesprochenen Themen bewegten sich im politischen Raum, wobei auffallend sei, dass etablierte Parteien kaum Interesse für das Thema der Überwachung zeigten, da sie gleichsam im selben Boot säßen, welches sie selbst in den vergangenen Jahren gesteuert hätten. Es gäbe daher keine großen Intentionen, das politische System in Bezug auf Überwachung grundlegend zu ändern. Sofern über eine Neuordnung des politischen Raumes diskutiert würde, stelle sich die Frage, ob Geheimdienste in ihrer jetzigen Verfassung als „Geheimgesellschaften“ für eine Neuordnung des politischen Raumes noch akzeptabel seien.

Hörer_in: Die Verantwortung der einzelnen Nutzer_innen sei in Erinnerung zu rufen, vor allem in Bezug auf die Unsitte ungelesen akzeptierter AGB. Daneben sei zu fragen, ob für den öffentlichen Raum des Internets nicht der gleiche Anspruch auf Schutz durch den Staat wie im öffentlichen Realraum bestehe.

LS: [an Vorredner_in] Einer Diskussion der Enquete-Kommission „Internet und digitale Gesellschaft“[62] sei zu entnehmen gewesen, dass die Realzeit zum Lesen aller pro Kopf durchschnittlich über die Lebenszeit akzeptierter AGB etwa 30 Jahre betrage. Dies verdeutliche die immense Überforderung der Nutzer_innen in Bezug auf datenschutzbewusstes Handeln, da es in Bezug auf dieses Beispiel praktisch in keiner Weise mehr möglich sei, sich mündig zu verhalten.[63]

Mod. RH: Die vergangenen Fragen konzentrierten sich auf die Thematik der Angreifbarkeit von Kryptographie; desweiteren auf das scheinbare Desinteresse der Politik an einer Neuordnung der Verhältnisse, woraus sich eine Linie zum Veranstaltungstitel[64] ziehen ließe, der den ausländischen Vorwurf eines „digitalen Analphabetismus“ in Bezug auf die hiesige Debatte aufnehme und damit die Frage stelle, was der Bildungsbereich in Deutschland zur Überwachungsproblematik beizutragen habe; schließlich wurde die Bedeutung der Verantwortung des Einzelnen sowie das Missverhältnis zwischen Entwickler_innen und Anwender_innen als Ursache unsicheren Verhaltens im digitalen Raum angesprochen. Herr Giessmann wurde um eine Stellungnahme gebeten.

EGG: Der Ausweg aus der Problematik um fehlerbehaftete Sicherheitsverfahren könne darin bestehen, gänzlich auf diese zu verzichten. Die Möglichkeiten zum Schutz von Nutzer_innen müssten im Gegenteil intensiv genutzt und nicht leichtfertig weggegeben werden, obwohl sie unvollkommen seien. Der Mangel an einfach bedienbaren Verschlüsselungsprogrammen sei auf das Versäumnis von Techniker_innen zurückzuführen, sich hinreichend über den Aspekt der einfachen Benutzbarkeit in der Entwicklung vorab zu verständigen. In der Internetkommunikation habe man es allerdings bspw. geschafft, die verschlüsselte Verbindung mit einer Webseite durch ein kleines Sicherheitsschloss-Symbol oder durch entsprechende Signalfarben zu verdeutlichen. Obgleich diese Kennzeichnungen

62 https://de.wikipedia.org/wiki/Enquete-Kommission_Internet_und_digitale_Gesellschaft (zuletzt aufgerufen: 03. Sep. 2015).

63 Anm. d. Pr.: Vgl. „1.1.1.1 Ausgestaltung von Nutzungsverhältnissen durch Allgemeine Geschäftsbedingungen“, in: »Zwölfter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft“«, Deutscher Bundestag, Drucksache 17/12540, 8, online abrufbar unter: https://digitalcourage.de/sites/default/files/users/161/12_verbraucherschutz.pdf – Kurzlink: http://kurzlink.de/5B6YcWfCX (zuletzt aufgerufen: 03. Sep. 2015).

64 Urspr. „Edward - der Whistleblower, der nichts enthüllt hat? Zum Vorwurf des "Digitalen Analphabetismus" im Jahr 1 nach Snowden“.

noch keinen hinreichenden Schutz gewährleisteten, stellten sie einen wichtigen Schritt auf dem Weg dar, digitale Kommunikation sicherer zu gestalten.

LS: Software, die zur Gewährleistung sicherer Kommunikation verwendet werde, komme häufig aus nicht-kommerziellen Bereichen (Open Source). Den Entwickler_innen gehe es dabei, da sie vorwiegend hierfür in ihrer Freizeit programmierten, hauptsächlich darum, die gewünschten Funktionen umzusetzen, ohne dabei auf möglichst einfache Bedienung achten zu müssen. Es sei für Entwickler_innen auch nicht nötig, ansprechend gestaltete Bedienoberflächen auszuarbeiten. Projekte wie „Pretty Easy Privacy“ zeigten zum einen den Versuch, komplexere Sicherheitsverfahren einfacher bedienbar zu gestalten, zum anderen aber auch die Gefahr, ein zentrales Anliegen von quelloffener Software zu unterwandern, nämlich, Technik nicht nur zu benutzen, sondern auch zu verstehen. In Bezug auf die Forderung nach Mündigkeit stelle sich die Frage, welches Maß an Vereinfachung auf der einen Seite notwendig, auf der anderen Seite schädlich sei. Diese Gratwanderung werde durch den folgenden Satz Albert Einsteins deutlich: „So einfach wie möglich, aber nicht einfacher.“ – dieser Gedanke sei ein angemessener Leitsatz in Bezug auf Softwareentwicklung. Eine Auslegung dieses Gedankens sei in der häufig anzutreffenden Differenzierung zwischen „Grundeinstellungen“ und „Erweiterten Einstellungen“ zu sehen, um gleichermaßen Einsteiger_innen wie fortgeschrittenen Nutzer_innen gerecht werden zu können. Ein inakzeptabler Zustand sei jedoch, Grundeinstellungen so zu gestalten, dass es für Nutzer_innen bspw. überaus frustrierend werde, die Einstellungen zur Privatsphäre überhaupt einfach auffinden zu können bzw. diese immer wieder neu setzen zu müssen.

Mod. RH: Aufruf für weitere drei Fragen aus der Hörer_innenschaft.

Hörer_in: [an EGG] Neben der angesprochenen Problematik um Zero Day Exploits hieß es, es sei noch kein modernes Verschlüsselungsverfahren gebrochen worden. Allerdings werde von einige modernen Verfahren abgeraten, weil diese als zu angreifbar gälten. Der Algorithmus SHA-1 sei ein Beispiel dafür.[65] Daher sei der These zu widersprechen, es sei noch kein modernes Verschlüsselungsverfahren gebrochen worden.

Hörer_in: Es hieß, Regierungen hätten ein Interesse daran, Daten zu sammeln, um eine Informationsübermacht zu erlangen. Wie könnten sich Bürger_innen unter dieser Betrachtung dann überhaupt mit der Forderung nach Schutz ihrer Grundrechte an ihre Regierung wenden, wenn diese doch offensichtlich andere Interessen verfolgten, als den Datenschutz von Bürger_innen zu gewährleisten?

In Bezug auf Facebook, welches eine Art Vorreiter einer neuen, offenen Welt gelte, dessen Gründer Mark Zuckerberg mit dem Spruch für Facebook werbe, „to make the world more open and connected“ [die Welt offener und in Verbundenheit gestalten], sei festzustellen, dass sich Nutzer_innen in diese neue Kultur der Anonymitätslosigkeit freiwillig begäben. Daraus ergebe sich die Frage, ob die Mehrheit der Bevölkerung an jenen klassischen Forderungen des Datenschutzes, der aktuell diskutiert werde, überhaupt noch interessiert sei. Die Frage stehe im Zusammenhang mit der Problematik, Überwachung in ihrer heutigen Form, vor allem durch das massenhafte Sammeln von Verbindungsdaten, in ihren

65 https://de.wikipedia.org/wiki/Secure_Hash_Algorithm#SHA-1 (zuletzt aufgerufen: 02. Okt. 2015).

potentiellen Auswirkungen der Mehrheit der Bevölkerung überhaupt wirksam verständlich machen zu können.

Hörer_in: Es gäbe eine Unsicherheit darüber, gegen wen genau sich Nutzer_innen in der Überwachungsaffäre überhaupt zur Wehr setzen sollten. Aktuell zeigten sich mindestens zwei Gegenspieler. Auf der einen Seite der Staat, auf der anderen Unternehmen und Konzerne. In Bezug auf letztere würden Nutzer_innen zu Produkten, bspw. In Form von personalisierter Werbung, gegen die es aktuell noch möglich sei, sich zur Wehr zu setzen bzw. die Mechanismen dieser Überwachung zu erkennen. In Bezug auf den Staat jedoch sei Gegenwehr ungleich schwieriger. Der Staat könne durch seine übergeordneten Befugnisse den verbliebenen Raum des Privaten immer weiter einschränken und habe dadurch immer Möglichkeiten, Bürger_innen zu überwachen.

EGG: [an Vorredner_in] Die These, kein modernes Kryptoverfahren sei bisher gebrochen worden, sei eine etwas provokante gewesen. Dennoch sei SHA-1, dessen Schwäche im Algorithmus inzwischen bekannt sei, nicht aus der Schwäche seines Algorithmus' heraus als schwach zu verstehen, sondern aufgrund der zu kurzen Schlüssellänge. SHA-1 sei eine Funktion, die von beliebigen Daten Prüfwerte (eine Art Fingerabdruck) erzeugen könne. Die geringe Größe des dabei entstehenden Prüfwertes sei die Schwäche dieser Funktion. Dieses Problem sei seit einigen Jahren bekannt, sodass Angriffe auf dieses Verfahren entwickelt worden, durch welche die Angriffskomplexität auf SHA-1 gesenkt wurde, sodass aktuell von der Verwendung von SHA-1 abgeraten werde. Dennoch gäbe es keinen öffentlich bekannten Beleg, der die Schwäche von SHA-1 in der Form nachweise, dass von zwei unterschiedlichen Datenmengen reproduzierbar der selbe Prüfwert erstellt worden sei. Erst unter diesen Bedingungen gelte SHA-1 als gebrochen. MD5 sei ein weiterer Algorithmus dieser Art mit vergleichbar problematischer Schlüssellänge, jedoch sei auch hier wie bei SHA-1, und darauf zielte die These des Vortrags ab, nicht der Algorithmus das Problem, sondern die Art und Weise der (infrastrukturellen) Benutzung desselben. Dies verdeutliche, dass ein in der Theorie sicheres Verfahren allein keinen Schutz biete, wenn es praktisch nicht angemessen angewendet werde.

Die Kontrollsucht des Staates, auch in Bezug auf die Idee, Hintertüren zu kaufen, sei bedrückend. Die Abhörtechniken von vor fünfzig Jahren erlaubten das Abhören mehr oder weniger nur aus Telefonzentralen heraus. Der Stand der Technik begrenze die Möglichkeiten zum Abhören, sodass heute eine Überwachung sehr viel umfänglicher arbeiten könne. Eine manipulierte Basisstation reiche, um sämtliche mit ihre verbundenen Mobiltelefone abzuhören. Ein Mittel gegen staatliche Überwachung fehle.

LS: [an EGG] Oft sei zu vernehmen, der Schutzauftrag des Staates bestehe darin, die Bevölkerung vor Lauschangriffen aus dem Ausland zu beschützen. Dieses Verständnis sei so nicht richtig. Der Schutzauftrag des Staates richte sich zunächst gegen sich selbst. Die Achtung der Bevölkerung stehe allerdings dabei vor dem Schutz der Bevölkerung. Somit bestehe die Hauptaufgabe des Staates eigentlich darin, die Bevölkerung vor dem Staat selbst zu schützen. Es sei unverständlich, warum diese Verfehlung des Staates an seinem eigenen Rechtfertigungsgrund die Bevölkerung nicht „auf die Barrikaden“ treibe. Bürger_innen stünden in der Verantwortung, darauf zu achten, dass der Staat seinen

Schutzauftrag auch erfülle. Die seit Jahren stattfindende „Freiheit statt Angst“-Demonstration verzeichne immer geringere Teilnehmerzahlen. Man könne nun diese Verantwortung von sich weisen, wodurch sich allerdings das Problem nicht beheben lasse, dass der Staat seiner Grundaufgabe der Bevölkerung gegenüber nicht mehr gerecht werde und Bürger_innen dieses Problem gar nicht mehr wahrnähmen. Dies spiele auf die Frage an, ob die Mehrheit der Bevölkerung an einem Schutz der Privatsphäre überhaupt noch interessiert sei. Ginge man von einem derartigen Desinteresse der Bevölkerung aus, gelte jedoch nach wie vor das Prinzip des Minderheitenschutzes. Sagten neun von zehn Bürger_innen, sie hätten nichts zu verbergen und ein Bürger meine darauf „ich aber schon“, so mache dieser sich verdächtig und sei folglich nach einem Mehrheitsprinzip nicht mehr geschützt. Diese Denkweise, Grundrechte von der Zahl der Interessent_innen abhängig zu machen, zerstöre den Minderheitenschutz und damit jenen Katalog an gesellschaftlichen Werten, der über Generationen hin hart erkämpft wurde.

Weitergedacht stoße man auf das Problem der Entmündigung, sobald eine Minderheit einer Mehrheit vorschreibe, welche Grundrechte diese wahrzunehmen hätte, gleichwohl sie an diesen kein Interesse habe. Hier stelle sich jedoch die Frage, ob dieses Desinteresse an Grundrechten überhaupt ausreichend reflektiert sei. Es könne nur dann von einer Entmündigung der Mehrheit durch eine datenschutzbewusstere Minderheit gesprochen werden, wenn die Mehrheit sich zuvor überhaupt mündig zu diesem Thema geäußert habe. Der status quo sei eher der einer Mehrheit, die sich mit der durchaus komplexen Frage nach der Relevanz von Grundrechten überhaupt nicht auseinandersetzen wolle. Entsprechend stelle sich die Frage, wie mit dieser Situation in Bezug auf Mündigkeit zwischen den folgenden Extrema zu verfahren sei, also entweder die Mündigkeit trotz mangelnder Auseinandersetzung anzunehmen und damit den Verlust von Datenschutzgrundrechten zu riskieren und auf der anderen Seite, die Selbstbestimmung zu ignorieren und Bürger_innen ein Interesse an Datenschutz mehr oder weniger aufzunötigen.

In Bezug auf Mark Zuckerberg sei auf das erwähnte Zitat hin ein weiteres Zuckerberg-Zitat in Erinnerung zu rufen: „They 'trust me' ... dumb fucks.“ [sie [Anm. d. Pr.: gemeint ist die Facebook-Nutzer_innenschaft] vertrauen mir, diese dummen Fotzen].[66] Dieses Zitat verdeutliche die Ambivalenz marktwirtschaftlicher Verwertung von Daten, die nicht davor zurückschrecke, in der Verpackung eines ehrwürdigen Ziels gegensätzliche Interessen zu verfolgen.

In Bezug auf die Frage, wer in der Überwachungsproblematik das böswillige Gegenüber sei, entwickele sich tatsächlich eine gesamtgesellschaftlich ungesunde Polarität zwischen Verschwörungstheorie und Gleichgültigkeit. Wichtig sei, die historisch lang gewachsenen Schutzmechanismen für Bürger_innen nicht leichtfertig für vermeintlich kostenlose Angebote aufzugeben, da dies keinem mündigen Verhalten entspräche.

Mod. RH: Aufruf zur abschließenden Fragerunde.

Hörer_in: Der in der bisherigen Diskussion angewandte Staatsbegriff sei problematisch. Der Staat sei in Bezug auf Überwachung nicht nur auf einen Geheimdienst zu reduzieren, der Bürger_innen feindlich

66 HALLIDAY, J.: „Facebook: Mark Zuckerberg college messages reveal steely ambition“, theguardian.com, 18. Mai 2012, online abrufbar unter: http://www.theguardian.com/technology/2012/may/18/mark-zuckerberg-college-messages – Kurzlink: http://kurzlink.de/moAlbhax (zuletzt aufgerufen: 02. Okt. 2015).

gesinnt sei, sondern eine Institution des gesamten Volkes und damit Entsprechung auch aller hier Anwesenden, mit gemeinsamer Basis durch ein Grundgesetz. Den Staat als Feind zu sehen, führe in eine Situation, die zu einer Problemlösung kaum beitragen könne und fördere Verschwörungstheorien. [Zuspruch aus der Hörer_innenschaft]

Hörer_in: Das größte Problem bestehe nicht darin, Bürger_innen für Widerstand zu mobilisieren, sondern die Gründe für die problematische Werteverschiebung von Freiheit zu Sicherheit zu erklären. Diese habe eventuell ihren Grund im unterschiedlichen Verständnis für die Vorgänge in der realen Welt auf der einen und für die in der virtuellen Welt auf der anderen Seite. Es sei bspw. einfacher, die Arbeitsweise der Polizei zu verstehen als die Arbeitsweise eines rein im virtuellen Raum agierenden Unternehmens. Aus dem Unverständnis über die Möglichkeiten des virtuellen Raums heraus erkläre sich die allgemeine Freigebigkeit, mit der Daten im virtuellen Raum preisgegeben würden.

Hörer_in: Die gängigen Argumente gegen das Recht auf Privatsphäre im gesellschaftspolitischen Diskurs seien Kinderpornographie und Terrorbedrohung, beide in medienwirksamer Publikation und entsprechend wirksam gegen jede Gegenposition. Folglich müssten die von LS eingangs erörterten Argumente, die das Interesse ausnahmslos aller Bürger_innen, mit dem Recht auf Privatsphäre etwas Essentielles einzufordern, beschrieben, entsprechend ebenso medienwirksam entfaltet werden.

EGG: [an Vorredner_in] Es sei in der Tat ein falscher Weg, den Staat zu dämonisieren und pauschal zu behaupten, dieser greife gegen Überwachung nicht ein. Der Elektronischen Personalausweises[67] bspw. habe eine Reihe an Vorbehalten erzeugt, allerdings seien Funktionen wie die Möglichkeit eines pseudonymen Zugangs[68] zu Dienstleistern, entworfen von Kolleg_innen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), durchaus mit einem hohen Anspruch an den Schutz für Bürger_innen entwickelt worden, nämlich die Möglichkeit, mittels des Personalausweis ein Mittel zu haben, mit dem sich sicher im Netz bewegt werden könne. Dieses Verfahren binde ein Pseudonym, unter dem sich im Internet bspw. Einkäufe abwickeln ließen, an den Personalausweis, nicht an den Besitzer desselben. Dieses Pseudonym gehe bei einem Austausch des Personalausweises entsprechend verloren und verkompliziere daher den Umgang mit diesem Sicherheitsverfahren. Dennoch sei dies ein Beispiel für einen Versuch des Staates, Bürger_innen im virtuellen Raum Schutzmöglichkeiten zu bieten.

Dagegen sei anderen staatlichen Institutionen der zuvor erwähnte Schutzgedanke für Bürger_innen kaum anzurechnen. Es gäbe Teile gewisser Institutionen, die sich verselbständigten und nur noch auf die Durchsetzung eigener Prozesse bedacht seien. Der ehemalige Bundesminister des Innern Manfred Kanther habe bspw. einmal auf einem Kongress gesagt, man habe seit hundert Jahren die Möglichkeit abzuhören und wolle deswegen auch keine Kryptographie haben, damit man weiter abhören könne.[69]

---

67 https://de.wikipedia.org/wiki/Personalausweis_%28Deutschland%29#Der_elektronische_Personalausweis_.28nPA.29 (zuletzt aufgerufen: 02. Okt. 2015).

68 https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Personalausweis/FAQ/FAQ_node.html#faq1529338 – Kurzlink: http://kurzlink.de/Rrv2TPqPK (zuletzt aufgerufen: 02. Okt. 2015).

69 Anm. d. Pr.: Vgl. KOSSEL, A.: „Datenschutz ade – Kanther fordert Krypto-Gesetz“, ct 6/97, online abrufbar unter: http://www.heise.de/ct/artikel/Datenschutz-ade-285626.html – Kurzlink: http://kurzlink.de/0XVGVEghT (zuletzt aufgerufen: 28. Aug. 2015).

LS: [an Vorredner_in] In der Überwachungsproblematik würden nur allzu häufig Freiheit und Sicherheit gegeneinander abgewogen. Diese Gegenüberstellung, Freiheit versus Sicherheit, sei jedoch wenig zielführend, da es sich hierbei um eine Kategorienverwechslung handle. Freiheit stehe auf einer anderen, nämlich übergeordneten Ebene als Sicherheit. Sicherheit werde erst durch Freiheit ermöglicht. Werde Freiheit aufgegeben, so gehe damit die Aufgabe dessen einher, was ein sicheres Leben in der Gesellschaft überhaupt erst ermögliche. Daher ließen sich beide Begriffe nicht gegeneinander aufwiegen. Zielführender als die Forderung nach Sicherheit sei die nach Frieden. Obgleich Sicherheit als Bedürfnis des gesamtgesellschaftlichen Lebens ein nachvollziehbares Anliegen sei, sei Sicherheit doch bei genauer Betrachtung nur das Vehikel zum letztlichen Wunsch der Allgemeinheit nach Frieden.

Hörer_in: [an Vorredner_in] Der These, Freiheit über Sicherheit zu stellen, sei zu widersprechen. Obgleich Freiheit durch Priorisierung von Sicherheit gefährdet werde, werde umgekehrt durch Priorisierung von Freiheit keinesfalls ein wünschenswertes Maß an Sicherheit erreicht.

LS: [an Vorredner_in] Die These habe darauf abgezielt, einen Bezug zu den erwähnten Argumenten, Überwachung diene bspw. der Prävention von Terroranschlägen, herstellen zu wollen. Das Argument der Terrorprävention arbeitete mit irrationaler Angst, denn es gäbe in Deutschland keinen Fall von Opfern durch Terrorismusanschläge. Der Gedanke an einen möglichen Terroranschlag, der Bürger_innen aus dem Nichts und in jeder Alltagssituation treffen könne, schüre eine Angst, welche die durchschnittliche Lebenserfahrung in einem Maß übersteige, dass sie zu einer geistig kaum mehr fassbaren Gefahr werde und aus diesem Grund viele Menschen in einem hohen Maß psychologisch beschäftige. Aus diesem Grund werde besonders die Terrorprävention immer wieder als Argument für Überwachung angeführt.

Eine ähnliche Betrachtung helfe in der Problematik des sorglosen Aufenthalts im wenig verstandenen virtuellen Raum. Für viele Nutzer_innen sei scheinbar der virtuelle Bereich aufgrund der Unverständlichkeit seiner Mechanismen psychologisch von größerer Anziehungskraft als der eher verständliche und damit weniger interessante Realraum.

In Bezug auf die Rolle des Staates und demnach das Verständnis über diesen sei festzuhalten, von den gewählten staatlichen Repräsentanten eigenverantwortlich und mit Nachdruck zu fordern, ihren Schutzauftrag der Bürger_innen nachzukommen, erfüllten sie ihn nicht. In der Verpflichtung zur Verantwortung zeige sich der durchaus bedeutende Horizont der Aussage der Hörer_in, der Staat bestehe aus allen Bürger_innen und sei keinesfalls ein Konstrukt, welches man als ein feindlich gesinntes Gegenüber von sich weisen könne. In diesem Zusammenhang erledige die sehr kleine politische Opposition in der Überwachungsfrage ihre Arbeit recht gut und müsse unterstützt werden, vor allem mit öffentlichen Bekundungen. Die politische Opposition benötige allerdings für diese Arbeit Unterstützung aus der Bevölkerung durch öffentlichen Protest. Die Teilnahme der Bevölkerung sei auf entsprechenden Demonstration, die LS besucht habe, zu gering gewesen.

Mod. RH: Abschluss der Diskussion, Verweis auf die Praxisveranstaltungen zur Kryptographie[70] und den Abschluss der Veranstaltungsreihe im Januar. Bitte um Werbung und Kritik per E-Mail. Danksagung

70 http://jahr1nachsnowden.de/veranstaltungen/pr2 (zuletzt aufgerufen: 02. Okt. 2015).

an die Gastredner_innen unter Applaus der Hörer_innenschaft. Dank an die Hörer_innenschaft für die kompetente Diskussion. Verabschiedung.

Studentische Initiative:
„Edward - der Whistleblower, der nichts enthüllt hat?
Zum Vorwurf des "Digitalen Analphabetismus" im Jahr 1 nach Snowden“
Theorieveranstaltung III – „Vom Sinn der Überwachung“ (09. Jan. 2015 – WiSe 2014/15)

Protokoll zur Abschlussveranstaltung „Vom Sinn der Überwachung“

Gastredner_innen:	Nele Trenner (NT)
	Dr. Anne Käfer (DrAK)
	Doris Aschenbrenner (DA)
Moderation:	Alexander Czekalla (Mod. AC)
Eröffnung, Moderation und Protokoll:	Roland Hummel (Mod. RH)

Initiatoren:	Amon Kaufmann (kaufmann@physik.hu-berlin.de)
	Roland Hummel (roland.hummel@theologie.hu-berlin.de)

Eröffnung

Aus gesundheitlichen Gründen könne der Mit-Initiator der stud. Initiative, Amon Kaufmann, an der Veranstaltung nicht teilnehmen. Ebenfalls krankheitsbedingt habe der geplante Gastredner Friedrich Schorlemmer seine Teilnahme kurzfristig absagen müssen. Unterstützung erhalte die Initiative durch den Deutschen Journalistenverband Berlin vertreten durch Alexander Czekalla, welcher den heutigen Abend in der Moderation unterstütze.

Nach der Eröffnung erfolge eine kurze Vorstellung der Gastredner_innen, welche daraufhin die Möglichkeit hätten, ihre Thesen nacheinander zu präsentieren. Es folge eine geschlossene Podiumsdiskussion von vierzig Minuten, welche nach einer zehnminütigen Pause für die Hörer_innenschaft zu einer fünfundvierzigminütigen, offenen Diskussion hin geöffnet werde (Folie 2)[71].

Thematisch stehe der Veranstaltungsabend in der Linie einer zunächst philosophischen Betrachtung der Auftaktveranstaltung im Nov. 2014, welche als Grundlage zur Überwachungsproblematik die Bedeutung der Privatsphäre untersuchte, sowie einer zweiten Veranstaltung im Dez. 2014, die sich mit den Möglichkeiten beschäftigte, Privatsphäre durch Kryptographie zu schützen (Folie 3). Die nun folgende gesellschaftspolitische Dimension der Überwachungsaffäre (Folie 4) zu diskutieren solle, trotz der aktuell medial sehr präsenten Probleme wie die Ebolafieber-Epidemie in Westafrika, den Bürgerkrieg in Syrien, die Ukraine-Krise, den Anschlag auf Charlie Hebdo in Paris oder in nationaler Hinsicht die PEGIDA-Bewegung, ein wichtiges, wenn nicht das wichtigste Anliegen gesellschaftspolitischer Debatten sein, da Überwachung Ausdruck einer ungesunden Demokratie sei. Ohne eine gesunde Demokratie könne es keine gesunden Problemlösungen geben. Dieser Gedanke stamme aus einem Beitrag des Deutschlandfunkes vom 4. Jan. 2015 (Folie 5): „Denn anlasslose Massenüberwachung, wie sie Geheimdienste heute ausüben, wirkt auf uns und unsere Demokratien genau wie eine Krankheit. Sie macht uns schwach.“[72]

71 Angaben der Folien dieses Abschnitts s. Anhang 5 »„Vom Sinn der Überwachung“ – Präsentationsfolien der Veranstaltung«.

72 KARIG, F.: „Staatliche Überwachung - Befallen vom Überwachungsvirus“, deutschlandfunk.de, 04. Jan. 2015, online abrufbar unter: http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639 – Kurzlink: http://kurzlink.de/zasSFYovB (zuletzt aufgerufen: 30. Aug. 2015).

Exkurs: „The Dark Knight“

Eines der größten Probleme der aktuellen Debatte bestehe darin, das Obskure der Überwachung visuell begreifbar zu machen (Folie 6). Ein interessanter Versuch der Visualisierung einer die Gesellschaft vollständig durchdringenden Überwachung finde sich in der neueren Hollywood-Verfilmungen des Comic-Helden „Batman“, der 2008er Produktion „The Dark Knight“ [„Der Dunkle Ritter“][73] (Folie 7). In der fiktiven Stadt „Gotham City“ trete der Held dieses Films, Batman, für Recht und Ordnung ein, wann immer die konventionelle Exekutive gegen einen übermächtigen Feind versage, der in diesem Fall in Form des Anti-Helden „Joker“ auftrete (Folien 8-9). Das einzig inhaltlich neue dieser klassischen „Gut gegen Böse“-Filmproduktion sei die Art und Weise, wie Überwachung als Instrument gegen den Terror des Anti-Helden thematisiert werde. Der Held Batman, welcher in der Nacht maskiert für das Gute kämpfe, sei bei Tage in unmaskiertem Auftreten Besitzer eines globalen Hochtechnologieunternehmens, wodurch es ihm möglich sei, eine Überwachungsmaschinerie zu entwickeln, die jedes Mobiltelefon der Stadtbevölkerung zu einem Abhörgerät umfunktioniere [Vgl. Abb. 1-2 u.]. Auf diese Weise sei er dazu fähig, jedes Ereignis der Stadt zu jeder Zeit wie auf einem Radarbild nachzuverfolgen (Folie 10). Obgleich es dem Helden mit Hilfe dieses Überwachungsapparates möglich sei, dem Terror des Anti-Helden Einhalt zu gebieten, kritisiere der engste Vertraute des Helden die Überwachungsmaßnahmen vehement als „unethisch“, „gefährlich“ und schließlich als „zu viel Macht für eine Person“.[74]

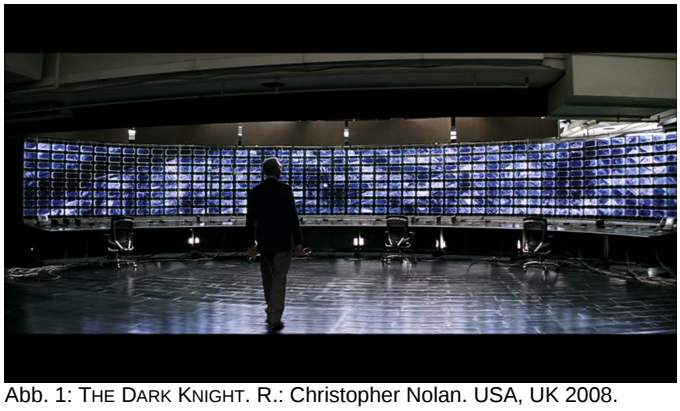


Abb. 1: THE DARK KNIGHT. R.: Christopher Nolan. USA, UK 2008. Zeitindex 01:51:10.

Abb. 2: THE DARK KNIGHT. R.: Christopher Nolan. USA, UK 2008. Zeitindex 02:03:59.

Bemerkenswert sei rückblickend eine Filmkritik der Berliner „taz.die tageszeitung“ (Folie 11), die 2008, fünf Jahre vor den Snowden-Enthüllungen, über das im Film thematisierte Zusammenspiel von Terrorismusbekämpfung und Überwachung ein Urteil fälle, welches nach den Snowden-Enthüllungen sicher in dieser Form nicht publiziert worden wäre, Zitat: „Die Anspielungen auf aktuelle Situationen des "War on Terror" nimmt man besser erst gar nicht ernst.“[75]

Vorstellung der Gastredner_innen

Doris Aschenbrenner sei Diplom-Informatikerin mit dem Schwerpunkt Robotik, netzpolitische Sprecherin der BayernSPD und arbeite am Zentrum für Telematik in Gerbrunn nahe Würzburg. Ihre Doktorarbeit

73 https://de.wikipedia.org/wiki/The_Dark_Knight (zuletzt aufgerufen: 19. Sep. 2015).

74 THE DARK KNIGHT. R.: Christopher Nolan. USA, UK 2008. Zeitindex 01:52:26-01:53:48.

75 SCHWEIZERHOF, B.: »"Batman"-Verfilmung "Dark Knight" – Das Sommergespenst«, taz.de, 30. Jul. 2008, online abrufbar unter: https://www.taz.de/!5178293/ (zuletzt aufgerufen: 19. Sep. 2015).

schreibe sie in der Thematik „Multi-Roboter-Systeme“. Zudem sei sie in Verbänden wie der Gewerkschaft für Erziehung und Wissenschaft (GEW) sowie auf Kongressen wie denen des Chaos Computer Clubs (CCC) aktiv.

Dr. Anne Käfer sei Dozentin im Fachbereich Systematische Theologie. Sie habe ihr Kirchliches Examen im Jahr 2001 absolviert und 2009 die Lehrbefugnis für das Fach Systematische Theologie erlangt. An der Humboldt-Universität sei sie erstmals 2011 Gastprofessorin gewesen; im selben Jahr habe sie ihre Arbeit als Referentin für Theologie und Kultur im Kirchenamt der Evangelischen Kirche in Deutschland aufgenommen. Aktuell lehre sie in Berlin und Leipzig. Neben Friedrich Schorlemmer sei sie eine der wenigen Theolog_innen, die sich öffentlich kritisch mit der Überwachungsproblematik auseinandersetzen.

Nele Trenne sei selbständige Rechtsanwältin mit dem Schwerpunkt Datenschutz. Sie berate Verbraucher_innen und Unternehmen in den Bereichen Datenverschlüsselung und Datensicherheit sowie im Bereich Arbeitnehmerschutz in den Themen Überwachung und Datennutzung für Werbezwecke. Sie halte einerseits Vorträge über die datenschutzproblematische Nutzung von Sozialen Medien, Arbeitsrecht und den Datenschutz in der Medizin sowie andererseits zur Sensibilisierung des Wertes persönlicher Daten für die Privatwirtschaft.

Eingangsthesen der Gastrednerinnen

Doris Aschenbrenner

Es sei nach Doris Aschenbrenner (DA) von immenser Bedeutung, die Problematik der globalen Überwachungsaffäre in der Diskussion zu halten. Aufgrund des politischen Umfelds und der größeren Netzszene sei die öffentliche Debatte in Berlin von anderer Dimension als in Würzburg. Die persönliche Wahrnehmung sei jedoch diejenige, dass über die Enthüllungen von Edward Snowden viel zu wenig gesprochen werde. Der Versuch des Wahlkampfes sei mit netzpolitischen Themen in Bayern besonders in ländlichen Regionen schwierig. Die persönlichen Hauptthemen DAs wie Informatik, „Digitaler Gesellschaftswandel“ und Überwachung durch Geheimdienste seien für die breite Bevölkerung wenig attraktiv. Persönliche Erfahrungen in der Durchführung von Anti-Vorratsdatenspeicherung-Demonstrationen zeigten, wie schwierig es sei, Bürger_innen für dieses Thema zu erreichen. Bei ihrem Vortrag bei der Arbeiterwohlfahrt in der unterfränkischen Kleinstadt Kitzingen zum Thema „Netzpolitik“ sei DA jedoch vom hohen Interesse der Rentner_innen am Thema Überwachung überrascht gewesen. Mit unerwarteter Diskussionsfreude habe die Hörer_innenschaft mit einem Durchschnittsalter jenseits von sechzig Jahren Meinungen zur Thematik eingebracht, wohl bedingt durch persönliche historische Erfahrungen mit diesem Thema. Jenseits dieser positiven Erfahrung von Aufklärungsarbeit werde das Thema Überwachung jedoch für die ihr innewohnende Brisanz nicht mit der nötigen Priorität in der Tagespolitik besprochen.

Hörer_in: Zwischenfrage, ob DA den Grund für das Desinteresse an der Überwachungsproblematik herausgefunden habe.

DA: [an Vorredner_in] Das Thema eigne sich zwar erstklassig als Einstieg in allgemeine Gespräche, sobald sich der Gedanke einer permanenten Überwachung in der Vorstellung der Gesprächspartner_innen jedoch realisiere, baue sich das ungute Gefühl einer „Paranoia“ auf, die eine weitere Auseinandersetzung mit dem Thema stark hemme. Die erste Hürde in der Thematik bestehe darin, den permanenten Überwachungszustand anzuerkennen. Dieser Gedanke erzeuge Angst, die eine weitere Auseinandersetzung äußerst unbequem mache. Der die Angst verursachende Gedanke werde folglich unterdrückt.

Selbst in den Reihen der Informatik sei mit Verwunderung auf das Ausmaß der enthüllten Überwachung reagiert worden. Dies erstaune im Zusammenhang mit dem Umstand, dass Überwachung im großen Stil unter Nutzung modernster Informationstechnologie nichts Neues sei, bedenke man die Enthüllungen um das weltweite Spionagenetz Echelon[76], welches Jahre vor den Snowden-Enthüllungen Gegenstand politischer Auseinandersetzung war.[77] DA erinnere sich, dass die von ihr in den neunziger Jahren gelesenen Online-Artikel über das Echelon-System seitens ihrer Angehörigen als unseriöse „Horrorgeschichten“ heruntergespielt wurden. Das Europaparlament habe sich zwar mit Echelon in einem Untersuchungsausschuss[78] befasst, die Auseinandersetzung sei jedoch im Zuge der Anschläge vom 11. Sep. 2001 auf das World Trade Center in New York zum Erliegen gekommen. Vielmehr sei im Zuge des politischen Kurses der Terrorismusbekämpfung dazu übergegangen worden, mit massiven personalen und finanziellen Aufwand Überwachungssysteme auszubauen. Der status quo an aktuellen Überwachungskapazitäten ermögliche es US-amerikanischen Geheimdiensten und ihren Partnern die Informationen aller bedeutenden Knotenpunkte des Internets in Echtzeit abzufangen, auszuwerten und zu speichern. Die für eine solche, auf pausenlosen Einsatz ausgelegte Überwachungstechnik versetze selbst IT-Fachkräfte in Erstaunen. Aus den gesammelten Informationen seien vor allem die Metadaten interessant, mittels derer sich durch Algorithmen gemeinsame Strukturen der Nutzer_innenschaft erkennen ließen. So sei es für einen Geheimdienst allein durch Metadaten-Analyse möglich, das Verhalten eines durchschnittlichen deutschen Bürgers an einem Freitagabend herauszufinden. Eine solche Analyse zeige dann, dass zu diesem Verhalten bspw. nicht der Besuch einer Hörsaalveranstaltung gehöre. Besucher_innen der aktuellen Veranstaltung fielen somit aus dem durchschnittlichen Verhaltensmuster und würden bereits dadurch auffällig. Problematisch werde es zudem für Menschen, die sich im Umfeld einer sog. Target- bzw. Zielperson aufhielten. DAs Arbeitgeber arbeite mit einem Unternehmen zusammen, welches nachweislich unter geheimdienstlicher Observation der NSA stehe, es also in diesem Fall um Wirtschaftsspionage und kaum um Terrorismusbekämpfung gehe. Es könne in diesem Zusammenhang nicht geleugnet werden, dass eine Absicherung gegen direkte Geheimdienstüberwachung wie die der NSA nicht zu realisieren sei, auch

76 https://de.wikipedia.org/wiki/Echelon (zuletzt aufgerufen: 19. Sep. 2015).

77 Anm. d. Pr.: Vgl. die Zeitpunkte der Veröffentlichung entsprechender Artikel bspw. In der Telepolis-Artikelsammlung zum Thema, online abrufbar unter: http://www.heise.de/tp/special/ech/default.html (zuletzt aufgerufen: 19. Sep. 2015).

78 SCHMID, E.: „Abhörsystem »Echelon«“, Pressebericht des Europaparlamentes A5-0264/2001 vom 05. Sep 2001, online abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?type=PRESS&reference=DN-20010905-1&format=XML&language=DE#SECTION1 – Kurzlink: http://kurzlink.de/YvoHYlXJo (zuletzt aufgerufen: 19. Sep. 2015).

wenn die betroffenen Unternehmen sich über Standards hinaus um Absicherung bemühten. Neben zwei deutschen Unternehmen sei aktuell Angela Merkel als Ziel von geheimdienstlicher Überwachung bekannt. Überwachung beträfe jedoch immer auch den Personenkreis einer Zielperson bis zum dritten Grad. Dies bedeute, dass auch all jene von Überwachung betroffen seien, die bspw. persönlichen Kontakt zu Angela Merkel hätten (1. Grad), dazu diejenigen, zu denen der erste Grad Kontakt habe (2. Grad) und der darauf folgende Personenkontaktkreis (3. Grad). Ein solcher Kreis an Überwachten umfasse eine stattliche Zahl an Personen, in deren Umfeld man überraschend schnell gelange. So wisse DA, dass sie selbst zum Kreis derer gehöre, die von der „three hops surveillance method“ [„Methode der Überwachung bis zum Personenkreis dritten Grades“] betroffen seien: DA habe die Telefonnummer ihres Landesvorsitzenden, dieser wiederum habe die Telefonnummer von Sigmar Gabriel, dieser wiederum die Telefonnummer von Angela Merkel, sodass sie theoretisch auch von der Überwachung durch Angela Merkel betroffen sei. Ähnliche Verbindungen entstünden recht schnell über den eigenen Chef oder den Präsidenten der eigenen Universität, da der Umfang eines Personenkreises dritten Grades immens sei.[79]

Der Ruf nach einer schnellen politischen Reaktion sei nachvollziehbar, jedoch schwer zu realisieren, besonders nicht durch anti-amerikanische Bestrebungen. Die Einrichtung eines NSA-Untersuchungsausschusses[80] sei eine positive Entscheidung des Bundestages gewesen. Die Europäische Union habe sich geweigert, einen ähnlichen Untersuchungsausschuss auf europäischer Ebene einzuberufen.[81] Im Zuge der Aufklärungsarbeit sei es zwar wichtig, Edward Snowden als Zeugen zu befragen, dieses Anliegen sollte jedoch nicht zentrales Thema der Untersuchungen sein. Wesentlich sei die Frage, wie internationale Beziehungen zu gestalten seien. In diesem Zusammenhang sei die schwache Reaktion der deutschen Regierung unter Berücksichtigung des Ausmaßes der globalen Überwachung irritierend und unverständlich. Wünschenswert wäre es, wenn Bürger_innen über einfach zu bedienende electronic countermeasures[82] [„elektronische Gegenmaßnahmen“] verfügten. Das Internet sei ebenso wie das Telefonnetz eine gewachsene Infrastruktur, die nicht auf Sicherheit ausgelegt worden sei und entsprechend machten sich Bürger_innen wenig Gedanken über die Absicherung dieser Kommunikationskanäle. Dies sehe man daran, wie lange es gedauert habe, bis das Konzept der Anti-Viren-Software in Computersystemen flächendeckend zum Standard geworden sei.

79 Anm. d. Pr.: Vgl. „Three degrees of separation: breaking down the NSA's 'hops' surveillance method“, theguardian.com, 28. Okt. 2013, online abrufbar unter: http://www.theguardian.com/world/interactive/2013/oct/28/nsa-files-decoded-hops – http://kurzlink.de/yqH8AONl0 (zuletzt aufgerufen: 17. Sep. 2015).

80 Beschluss des Bundestages über die Einsetzung eines Untersuchungsausschusses vom 18. Mrz. 2014, online abrufbar unter: http://dip21.bundestag.de/dip21/btd/18/008/1800843.pdf – Kurzlink: http://kurzlink.de/QFsRCe7f9 (zuletzt aufgerufen: 17. Sep. 2015).

81 Anm. d. Pr.: Vgl. aus dem "ENTWURF EINER ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS zu der Lage der Grundrechte in der Europäischen Union (2013–2014)" des Europäischen Parlaments vom 16. Juli 2015: "Das Europäische Parlament, [...] Bm. in der Erwägung, dass die Kommission und die Mitgliedstaaten auf die von Edward Snowden enthüllte massenhafte Ausspähung der Kommunikation über Internet und Telekommunikation im Rahmen des NSA-Programms „Prism“, das auch Daten aus europäischen Staaten einbezieht, kaum reagieren und nur geringe Bemühungen unternommen haben, um die Einhaltung der für europäische Bürger und für sich in der EU aufhaltende Bürger von Drittstaaten geltenden Schutzstandards durchzusetzen; […]", online abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2015-0230&format=XML&language=DE#title1 -- Kurzlink: http://kurzlink.de/xdbIA2nrX (zuletzt aufgerufen: 02. Okt. 2015).

82 https://de.wikipedia.org/wiki/Elektronische_Gegenma%C3%9Fnahmen (zuletzt aufgerufen: 19. Sep. 2015).

Verschlüsselungsverfahren müssten nun ebenso zum Standard werden, um die flächendeckende Überwachung zumindest zu erschweren.

Dr. Anne Käfer

Die Überwachungsaffäre sei nach Dr. Anne Käfer (DrAK) eine Thematik, deren Bearbeitung auch aus geisteswissenschaftlicher und theologischer Sicht erfolgen und vertieft werden müsse. Nach DrAk müsse das zentrale Anliegen für ein überwachungsfreies Internet und Telefon auf die Forderung „Geben Sie Gedankenfreiheit.“ abzielen. Es sei lange her, dass dieser Ausruf eine Forderung gewesen sei, bedenke man, dass die Freiheit, sich Gedanken zu machen, zu äußern und diese auszutauschen, in einer freiheitlich geordneten Demokratie als eine gesellschaftliche Selbstverständlichkeit gelte. Die Forderung „Geben Sie Gedankenfreiheit.“ aus Schillers „Don Karlos“ sei jedoch leider alles andere als veraltet.[83] Ein seltsames und eindrückliches Bsp. der Überwachung von Gedanken sei im Märchen „Meister Floh“ des Berliner Dichters E. T. A. Hoffmann zu finden. Diese vor fast 200 Jahren erschienene Erzählung enthalte eine Episode über die vermeintliche Entführung einer Frau, die dem Protagonisten angelastet werde, obgleich sich herausstelle, dass gar keine Frau vermisst werde. Dies halte die Figur des Geheimen Hofrats Knarrpanti jedoch nicht davon ab, dennoch nach einem Entführer zu suchen, da er die Auffassung vertrete, dass, „[...] sei erst der Verbrecher ausgemittelt, sich das begangene Verbrechen von selbst finde“.[84] So werde der Protagonist Peregrinus Tyß als Verdächtiger verhaftet und sämtliche persönliche Niederschriften, die sich in dessen Wohnung befänden, zwecks Sichtung durch die Behörden beschlagnahmt. In einem Tagebuch des Protagonisten finde sich ein scheinbarer Verdacht, der dem Stadtrat vorgelegt werde: „Die Stelle in dem Tagebuch, auf welche der weise Geheime Hofrat Knarrpanti den Abgeordneten des Rats aufmerksam machte, lautete: »Heute war ich leider *mord*faul.« – Die Silbe *mord* war dreimal unterstrichen, und Knarrpanti meinte, ob jemand wohl verbrecherischere Gesinnungen an den Tag legen könne, als wenn er bedauere, heute keinen Mord verübt zu haben!“[85] Diese Argumentation sei ausreichend, den Helden des Märchens schließlich zu verhaften. Geäußerte Gesinnungen und Gedanken, die der Protagonist in seinem gänzlich privaten Raum, in diesem Fall in seinem Tagebuch, äußerte, führten zur Einschränkung seiner äußeren Freiheit und so zur Aufgabe der Gedanken- und Meinungsfreiheit.

Gedankenfreiheit sei jedoch nicht nur eine Forderung der beiden Protestanten E. T. A. Hoffmann und Friedrich Schiller, sondern auch eine Forderung Martin Luthers in dessen Schrift „Von weltlicher Obrigkeit“. Die Annahme „Gedanken sind zollfrei“ solle, so führe Luther aus, von der Staatsmacht geachtet und geschützt werden.[86] Schutz von Gedankenfreiheit sei ein genuin protestantisches

83 Vgl. SCHILLER, F.: „Don Carlos, Infant von Spanien“ (1787), Kapitel 16, Zehnter Auftritt, online abrufbar unter: http://gutenberg.spiegel.de/buch/don-carlos-infant-von-spanien-3338/16 (zuletzt aufgerufen: 19. Sep. 2015).

84 Vgl. HOFFMANN, E. T. A.: „Meister Floh – Ein Märchen in sieben Abenteuern zweier Freunde“ (1822), Viertes Abenteuer, online abrufbar unter: http://gutenberg.spiegel.de/buch/meister-floh-3115/5 (zuletzt aufgerufen: 19. Sep. 2015).

85 Ebd., Fünftes Abenteuer.

86 LUTHER, M.: „Von weltlicher Obrigkeit, wie weit man ihr Gehorsam schuldig sei“ (1523), Kapitel 2, online abrufbar unter: http://gutenberg.spiegel.de/buch/von-weltlicher-obrigkeit-wie-weit-man-ihr-gehorsam-schuldig-sei-267/2 – Kurzlink: http://kurzlink.de/zvoCleLD0 (zuletzt aufgerufen: 28. Aug. 2015).

Anliegen. Martin Luther habe selbst auf dem Reichstag zu Worms unter Berufung auf sein Gewissen den Widerruf der in seinen Schriften geäußerten Gedanken verweigert.

Nele Trenner

Die aktuelle Politik zeige widersprüchliche Bestrebungen, freiheitliche Strukturen durch den Ausbau von Überwachung schützen zu wollen. Es sei schwer nachvollziehbar, dass den Fürsprecher_innen die einer solchen Politik innewohnende Widersinnigkeit derartiger Bestrebungen nicht auffalle. Dies werde bspw. an Äußerungen wie denen des Innenministers Thomas de Maizière deutlich, welcher dafür plädiere, zur Terrorismusbekämpfung Überwachung in anonymen Räumen des Internets auszubauen.[87] Die aktuelle Überwachung der Gesellschaft erfolge zum einen unfreiwillig durch eigene und fremde Regierungen, zum anderen in freiwilliger Form bspw. durch Nutzung von Smartphones verbreiteter Systeme wie denen von Google und Apple. Sei es durchaus möglich, sich der freiwilligen Überwachung zu entziehen, gäbe es hingegen keine Möglichkeiten, sich der unfreiwilligen Überwachung zu entziehen. Es stelle sich in der Konsequenz daraus erstens die Frage, ob gegen diesen Zustand etwas unternommen werden *wolle* und zweitens, ob dagegen etwas unternommen werden *könne*. Der NSA-Untersuchungsausschuss versuche in diesem Zusammenhang zumindest, Aufklärungsarbeit in Bezug auf Ausmaß und Umfang der Überwachung zu leisten. Die Äußerungen des Vorsitzenden Patrick Sensburg, die vorhandenen Beweise der Überwachung durch ausländische Geheimdienste nicht als ausreichend für Ermittlungsverfahren anzuerkennen, seien sehr besorgniserregend.[88]

In der Diskussion begegne man häufig der Argumentation, die Überwachung in Deutschland durch ausländische Geheimdienste sei durch mangelnde völkerrechtliche Souveränität der BRD bedingt. Entsprechende Diskussionen über dieses Thema hätten das Potential, sich in ihnen schnell verlieren zu können. NT widerspreche der These, Deutschland sei kein souveräner Staat. Entsprechende Behauptungen entstünden durch unzureichende Betrachtung jener Quellen, die zu derartigen Argumentation herangezogen würden.[89] In staatsrechtlichem Sinne sei Deutschland in jedem Fall ein souveräner Staat. Es könne jedoch durchaus die Frage gestellt werden, ob Deutschland sich in nicht-staatsrechtlichem Sinne souverän verhalte. Diesbezüglich lasse sich recht plausibel die These vertreten, Deutschland begebe sich freiwillig in die Abhängigkeit anderer Staaten. Dieses Abhängigkeitsgefüge, das einherginge mit der freizügigen Herausgabe von geheimdienstlichen Informationen über die eigene Bevölkerung, werde begründet mit der unumgänglichen Aufrechterhaltung internationaler freundschaftlicher Beziehungen. Es gelte nun, gegen die sich ausbreitende Überwachung aktiv zu werden.

87 „Innenminister: Das Internet, unkontrollierte Weiten - da hilft nur Polizei“, heise.de, 10. Dez. 2014, online abrufbar unter: http://www.heise.de/newsticker/meldung/Innenminister-Das-Internet-unkontrollierte-Weiten-da-hilft-nur-Polizei-2486053.html – Kurzlink: http://heise.de/-2486053 (zuletzt aufgerufen: 19. Sep. 2015).

88 Anm. d. Pr.: Vgl. Interview "Wir brauchen hieb- und stichfeste Beweise", deutschlandfunk.de, 30. Mai 2014, online abrufbar unter: http://www.deutschlandfunk.de/nsa-ermittlungsverfahren-wir-brauchen-hieb-und-stichfeste.694.de.html?dram:article_id=287802 – Kurzlink: http://kurzlink.de/W42g1OUIn (zuletzt aufgerufen: 19. Sep. 2015).

89 Anm. d. Pr.: Vgl. Interview „Die USA dürfen Merkel überachen“, zeit.de, 25. Okt. 2013, online abrufbar unter: http://www.zeit.de/politik/deutschland/2013-10/nsa-uerberwachung-merkel-interview-foschepoth/komplettansicht – http://kurzlink.de/IR4Mev0IR (zuletzt aufgerufen: 19. Sep. 2015).

Geschlossene Podiumsdiskussion

Abkürzungen der Namen:
NT: Nele Trenner
DrAK: Dr. Anne Käfer
DA: Doris Aschenbrenner
Mod. AC: Alexander Czekalla (Moderation)
Mod. RH: Roland Hummel (Moderation)

Mod. RH: [an DrAK] Die Überwachungsaffäre habe die Wirklichkeit der Überwachungspraxis als eine historisch kontinuierliche Größe gezeigt. Könne angesichts des nachweislich tiefgreifenden Interesses der Geheimdienste an jeder noch so banalen E-Mail die Meinungs- und Gedankenfreiheit noch als ein Bestandteil unseres gesellschaftlichen Wertekanons betrachtet werden?

DrAK: Entsprechend der Eingangsthese sei von einer starken Einschränkung der Meinungs- und Gedankenfreiheit auszugehen. Zwar sei nicht davon auszugehen, dass der unausgesprochene Bereich der Gedanken, also die noch ungeäußerten, rein gedanklichen Überlegungen, einer Überwachung unterlägen, allerdings sei ein Gedanke ja erst dadurch realisiert, dass er kommuniziert werde. Dieser Bereich der Kommunikation außerhalb der eigenen Person sei allein schon durch die Vorstellung einer potentiell möglichen Überwachung eingeschränkt. Kommunikation sollte hingegen ohne die potentielle Möglichkeit von weiteren Mithörer_innen möglich sein. Freier kommunikativer Austausch sei für verschiedenste Bildungsfortschritte von zentraler Bedeutung, bspw. für die Reflexion des Gewissens oder religiöser Sichtweisen. Das persönliche Kommunikationsverhalten DrAKs habe sich in Bezug auf die Möglichkeit ungehemmter Meinungsäußerung durch die aktuelle Überwachungsdebatte sehr eingeschränkt, sodass bspw. nicht mehr jeder Gedanke per E-Mail geäußert werde.

Mod. AC: Der Eingangsthese DAs sei zu entnehmen gewesen, jede Nachricht könne durch Geheimdienste abgefangen werden. DrAK habe zugegeben, nicht mehr jeden Gedanken in einer E-Mail zu äußern. Daher ergebe sich die interessante Frage an DA, DrAK und NT, wie hoch der persönliche „Grad an Paranoia“ eingeschätzt werde.

DA: Bedingt durch den Besuch auf dem erst kürzlich veranstalteten Chaos Communication Congress[90] sei der persönliche „Grad an Paranoia“ aktuell recht hoch. Die Frage sei, wieviel dieser „Paranoia“ praktische Konsequenzen habe, das eigene Nutzungsverhalten in Bezug auf digitale Medien anzupassen. Den eigenen Computer abzusichern läge noch im Bereich des Möglichen, bedeute aber schon Einschränkungen in der Kommunikation mit Kolleg_innen und Projektpartner_innen. Die Benutzung eines Smartphones sei hingegen nicht mehr möglich, da aus technischer Sicht aktuell kein handelsübliches Smartphone „NSA-sicher“ einzurichten sei. Spätestens der Verzicht auf ein Smartphone schränke die aktuelle Lebensqualität derart ein, dass ein Verzicht darauf nicht in Frage käme und so in der Konsequenz ein Stück Freiheit zugunsten von Lebensqualität aufgegeben werde. Ähnlich verhalte es sich mit der Entscheidung zwischen bedienbarer und sicherer Software. Entsprechend sei die angesprochene „Paranoia“ im Kopf immer höher als die tatsächlich gelebte. Der einzig wirklich sichere Computer sei demnach der im Keller stehende und deaktivierte. Ein gewisser

90 https://de.wikipedia.org/wiki/Chaos_Communication_Congress (zuletzt aufgerufen: 20. Sep. 2015).

Unsicherheitsfaktor müsse immer eingestanden werden und das persönliche Sicherheitsniveau entsprechend der eigenen langfristigen Möglichkeiten reflektiert werden. Persönlich attestiere sich DA eine gewisse Inkonsequenz in Bezug auf Maßnahmen gegen Überwachung: Es gäbe für sie durchaus mehr Möglichkeiten, das eigene Nutzungsverhalten sicherer zu gestalten, jedoch sei der Mehraufwand diesbezüglich mit einem für sie unzumutbaren Verlust an Bedienkomfort verbunden, sodass entsprechende Absicherungsmaßnahmen nicht umgesetzt würden.

DrAK: Auch bei DrAK sei der Grad an „Paranoia“ durch die Auseinandersetzung mit den Ereignissen der Überwachungsaffäre recht hoch. Dazu käme jedoch zudem der Umstand der Unkenntnis bzgl. geeigneter Schutzmaßnahmen, obgleich der Wille, das eigene Nutzungsverhalten anzupassen, vorhanden sei.

NT: [an DrAK] Bürger_innen, deren technisches Wissen für entsprechende Gegenmaßnahmen noch nicht ausreichend sei, die sich aber dennoch mit der Materie der Überwachung auseinandersetzten, seien besonders von „Paranoia“ belastet, bedingt durch das Wissen um die Überwachung bei gleichzeitiger Ohnmacht, dagegen etwas unternehmen zu können. Bereits der Schritt, eine E-Mailverschlüsselung einzurichten, sei ein aufwändiger, auf den allerdings zudem das Problem folge, dadurch nicht das Auslesen von Metadaten zu verhindern, da E-Mailverschlüsselung nur die Inhalte einer Nachricht schütze, nicht aber Absender- und Adressangaben. Diese unverschlüsselten Metadaten reichten jedoch allein schon für umfangreiche Überwachung aus: Werde bspw. ein Psychiater angerufen, sei nicht der Inhalt des Gesprächs interessant, sondern die Tatsache des Anrufs überhaupt. Diese Information könne anschließend mit weiteren verknüpft werden. Erfolge bspw. auf den Anruf beim Psychiater ein weiterer Anruf bei einer Online-Apotheke mit der Bestellung von Medikamenten, deren Substanzen sich, der Theorie nach, fernab primärer Verwendungszwecke auch für kriminelle Machenschaften verwenden ließen, ergebe die Metadaten-Analyse in der Verknüpfung „Anruf bei einem Psychiater“ und „Bestellung von potentiell gefährlichen Substanzen“ ein Bild, welches unberechtigt, aber mit schweren Folgen einen Alarm auslösen könne. Entsprechend sei auch bei NT der selbst empfundene Grad an „Paranoia“ hoch, verbunden mit der Selbsteinschätzung, zu wenig an aktiven Abwehrmöglichkeiten umzusetzen, da die technischen Hürden oft als zu hoch empfunden würden. Es ergebe sich die Frage, wer diesbezüglich zur Verantwortung gezogen werden müsse. Eine gewisse Eigenverantwortung müsse Bürger_innen abgewonnen werden. Gegen Überwachung jedoch müsse der Staat schützen.

DA: Der Grad der persönlichen „Paranoia“ könne von Bürger_innen selbst dadurch eingeschätzt werden, indem sie selbst einmal einschätzten, wie freizügig sie im Zuge der Überwachungsaffäre noch mit Suchanfragen in gängigen Suchmaschinen wie Google umgingen. DA sei diesbezüglich übervorsichtig geworden.

Mod. RH: Das beschriebene Verhalten, Suchbegriffe im Internet aufgrund von Überwachung anzupassen, könne durch verschiedene Studien als ein gesellschaftliches Phänomen nachgewiesen

werden.[91] [An DA] Worin bestehe aktuell die Bedeutung von Ausdrücken wie „Partnerschaft“ und „Freundschaft“ im Kontext der Politik von Regierungen, die sich gegenseitig überwachten?

DA: Diese Begriffe seien nicht mehr als gängige diplomatische Ausdrucksweisen in der Außenpolitik. Obgleich sie nicht im Bereich Außenpolitik tätig sei, eröffneten sich Politiker_innen durch Begriffe wie Partnerschaft und Freundschaft einen Formulierungsspielraum, der eine Gesprächsbereitschaft und Offenheit signalisiere. Diese Bedeutungen seien daher von jenen zu unterscheiden, die mit besagten Begriffen im privaten Bereich verbunden würden. Ähnlich verhalte es sich in der Kommunikation zwischen Unternehmen, die trotz eingegangener „Partnerschaften“ mit anderen Unternehmen nach wie vor mit diesen in Konkurrenz stünden. Formulierungen wie „deutsch-amerikanische Freundschaft“ seien demnach Ausdruckweisen der Diplomatie. Diese Formulierungen seien allerdings alles anderes als nutzlos, da sie auch Staaten in ungünstigen gegenseitigen Beziehungen Gespräche eröffneten. Daneben müssten jedoch auch die sehr unterschiedlichen Weltvorstellungen der Staaten, bspw. denen des europäischen und nordamerikanischen Raumes, berücksichtigt werden, die sich auf sprachliche Wendungen auswirkten. Ebenso verhalte es sich mit Politiker_innen unterschiedlicher Bereiche. Bezüglich der innenpolitischen Frage „Freiheit versus Sicherheit“ bspw. sei die Beurteilung dieser Frage sehr davon abhängig, ob Innenpolitiker_innen eher aus dem Bereich der Exekutive wie Polizei und BKA kämen oder aber bspw. aus der Informatik. Aus persönlicher Erfahrung wisse DA, wie schwer es sei, zwischen Politiker_innen unterschiedlicher Ausbildung ein angemessenes Miteinander in der Diskussion zu erreichen.

Härtere Umgangsformen in der internationalen Politik, bspw. eine Drohung Deutschlands gegenüber den USA, hätten am Ende keinerlei Mehrwert. Es habe die Möglichkeit bestanden, das geplante internationale Handelsabkommen TTIP als „Hebel“ gegen die USA einzusetzen, also die Verhandlungen zum gemeinsamen Wirtschaftsmarkt nur unter der Bedingung einer Aufklärung der Überwachungsaffäre weiterzuführen.

Mod. RH: [an NT] Welchen Preis zahle Deutschland für die Partnerschaft mit dem angloamerikanischen Raum, nicht nur bzgl. des Datenaustausches, sondern auch hinsichtlich der Duldung ausländischer Spion_innen in Deutschland als Gegenleistung für ausländische Geheimdienstinformationen?

NT: Der Blick auf die nationalen Nachteile durch internationale Überwachung dürfe nicht zu einseitig sein. So spionierten zum einen keinesfalls die Vereinigten Staaten von Amerika nur Deutschland aus, sondern auch jedes andere Land. Diese Länder spionierten wiederum im Rahmen ihrer Möglichkeiten ebenso jedes andere Land aus. Entsprechend sei Deutschland ein Teil dieses internationalen Überwachungsgefüges. Deutschland bezahle für die eigenen Überwachungsmaßnahmen einen immens hohen Preis, da Bürger_innen das Vertrauen in den Staat als beschützende Instanz und Garant der Grundrechte verlören. Langfristig schade dies dem Grundgesetz und damit der Gesellschaft insgesamt.

91 Vgl. WEIDEMANN, S.: „Freiheit unter Beobachtung?“, bpb.de, 25. Apr. 2014, online abrufbar unter: http://www.bpb.de/apuz/183084/freiheit-unter-beobachtung?p=all – Kurzlink: http://kurzlink.de/1pvJX5Z6L (zuletzt aufgerufen: 26. Aug. 2015).

Mod. RH: Es folge ein theologischer Blickwechsel. Frau Käfer sei neben Werner Thiede[92] und Friedrich Schorlemmer[93] eine der wenigen Theolog_innen, die sich kritisch mit digitaler Vernetzung auseinandergesetzt habe. In Bezug auf die Überwachungsaffäre habe sie in einem ihrer Beiträge geschrieben: „Dem protestantischen Christenmenschen kann es nicht gleichgültig sein, wie der Staat die Gedankenfreiheit der Staatsbürgerinnen und -bürger behandelt.“[94] [An DrAK] Worin bestehe die Begründung für diese Schlussfolgerung?

DrAK: Die zentrale lutherische Einsicht bestehe in der Erkenntnis, jeder Mensch könne in unmittelbarer Beziehung zu seinem Schöpfer stehen, also ohne die Notwendigkeit vermittelnder oder Gott gnädig stimmender Instanzen in dieser persönlichen Beziehung. Diese Beziehung bestehe in einer Kommunikation zwischen Mensch und Gott. Das Gewissen sei dabei nach Luther der Ort, an welchem der Mensch mit seinem Schöpfer in Kontakt stehe. Dieser Raum des Gewissens müsse nach Luther frei sein. „Frei“ bedeute in diesem Zusammenhang den Ausschluss fremder menschlicher Einflussnahme. Dies bedeute, dass keine menschliche Instanz darüber eine Macht haben und ebenso nicht darüber verfügen dürfe, was im Raum des Gewissens verhandelt werde. Dies betreffe z. B. Vorschriften darüber, was ein Mensch für falsch oder richtig zu halten habe. Dies spreche nicht gegen die Verständigung über Gewissensinhalte in menschlicher Gemeinschaft, sondern solle die Freiheit unterstreichen, sich um der eigenen Reflexion willen zwischenmenschlich über Gedanken, Überlegungen und Gesinnungen auszutauschen. Diese Verständigungsprozesse über Gewissensinhalte müssten nach Luther geschützt sein. Dieser Anspruch lasse sich bereits aus dem vollständigen Titel der Lutherschen „Obrigkeitsschrift“ ableiten: „Von weltlicher Obrigkeit, wie weit man ihr Gehorsam schuldig sei“.[95] Am Titel sei zu erkennen, wie wichtig Luther es sei, die Grenzen staatlicher Macht aufzuzeigen. Die Grenze sei demnach dort zu ziehen, wo der Bereich der Gewissensfreiheit und des freien Austausches über Gesinnungsinhalte beginne. Die Aufgabe des Staates bestehe darin, Leib und Gut zu schützen: „Das weltliche Regiment hat Gesetze, die sich nicht weiter erstrecken als über Leib und Gut und was äußerlich auf Erden ist.“[96] Dieser Schutz habe jedoch seinen Zweck darin, freie weltanschauliche Kommunikationsvorgänge unter den Menschen zu ermöglichen.

Mod. RH: Es gäbe durchaus Situationen, in denen lückenlose Überwachung in Alltagssituationen wünschenswert wäre. Bedenke man bspw. die Bahnsteige der Berliner U-Bahn mit ihrer gefühlt

---

92 Vgl. THIEDE, W.: „Die Kirche und der Zug der Digitalisierung“, in: Deutsches Pfarrerblatt 09 / 2014, online abrufbar unter: http://www.pfarrerverband.de/pfarrerblatt/index.php?a=show&id=3670 – Kurzlink: http://kurzlink.de/hTqfCFkQK (zuletzt aufgerufen: 28. Aug. 2015).

93 Vgl. POKATZKY, K.: „Recht auf Privatheit“, deutschlandradiokultur.de, 09. Dez. 2013, online abrufbar unter: http://www.deutschlandradiokultur.de/widerstand-recht-auf-privatheit.954.de.html?dram:article_id=271520 – Kurzlink: http://kurzlink.de/rOBtLsqvG (zuletzt aufgerufen: 28. Aug. 2015).

94 KÄFER, A.: „Freiheit oder Sicherheit?“, in: Deutsches Pfarrerblatt 04 / 2014, online abrufbar unter: http://www.pfarrerverband.de/pfarrerblatt/index.php?a=show&id=3583 – Kurzlink: http://kurzlink.de/dtUIJSMSi (zuletzt aufgerufen: 28. Aug. 2015).

95 LUTHER, M.: „Von weltlicher Obrigkeit, wie weit man ihr Gehorsam schuldig sei“ (1523), online abrufbar unter: http://gutenberg.spiegel.de/buch/von-weltlicher-obrigkeit-wie-weit-man-ihr-gehorsam-schuldig-sei-267/1 – Kurzlink: http://kurzlink.de/Y66nHgHlJ (zuletzt aufgerufen: 28. Aug. 2015).

96 LUTHER, M.: „Von weltlicher Obrigkeit, wie weit man ihr Gehorsam schuldig sei“ (1523), Kapitel 2, online abrufbar unter: http://gutenberg.spiegel.de/buch/von-weltlicher-obrigkeit-wie-weit-man-ihr-gehorsam-schuldig-sei-267/2 – Kurzlink: http://kurzlink.de/zvoCleLD0 (zuletzt aufgerufen: 28. Aug. 2015).

lückenlosen Kameraüberwachung, stelle sich die Frage, warum es keine Konsequenzen für Regelübertretungen, bspw. das Rauchen auf den Bahnsteigen, gebe. Dies betreffe ebenso randalierende Personen, Taschendieb_innen und die Frage, ob sich das eigene Fahrrad am Ende des Tages noch am selben Ort befinde. Bürger_innen profitierten von Überwachung demnach nicht einmal in Situationen, in denen Überwachung wünschenswert wäre. [An NT] Für wie lückenlos könne daher die Überwachung in Deutschland tatsächlich eingeschätzt werden?

NT: Bezüglich der U-Bahnstationen sei zunächst interessant, mit welcher Begründung auf die Videoüberwachung hingewiesen werde. Diese laute „zu ihrer Sicherheit“. Hinweise der Form „Dieser Bahnhof wird zu ihrer Sicherheit videoüberwacht“ erzeugten die Erwartung, jemand säße hinter der Videokamera, könne so auf Gefahrensituationen unmittelbar reagieren und bspw. Sicherheitspersonal entsenden, um Taschendieb_innen festzusetzen. Gemeint sei mit diesem Hinweis jedoch lediglich eine mögliche Erleichterung der Aufklärungsarbeit für jene Zwischenfälle, bei der es zu einer Aufklärung komme. Demzufolge werde nicht „zu ihrer Sicherheit“ überwacht, sondern allerhöchstens, um unter gewissen Umständen einen Aufklärungsprozess zu unterstützen. Die Befürchtung, ob Überwachungsdaten, die aktuell für einen bestimmten Zweck gesammelt würden, in Zukunft nicht auch für völlig andere Zwecke ge- und missbraucht werden könnten, unterstreiche das Gefahrenpotential von Überwachung. Ein solches Missbrauchspotential werde bspw. bei der Maut[97] deutlich. Dieses primär für den Einzug von Straßennutzungsgebühren entwickelte System erlaube es über die Erfassung der Nummernschilder exakt, die Routen der Fahrzeuge zu protokollieren. Dieses Missbrauchsargument sei eventuell punktuell unerheblich, da verständlich sei, dass ein solches Gebühreneinzugssystem die Fahrzeuge schließlich auch erfassen müsse. Ein einmal entsprechend errichtetes Erfassungssystem könne aber in Zukunft auch für Zwecke genutzt werden, die ursprünglich nie befürwortet worden wären. Die Möglichkeit dafür sei durch verschiedenste Systeme möglich, die zusammen bereits aktuell ein nahezu lückenloses Erfassen von Individuen ermöglichten.

DA: Aus einem Gespräch über Vorratsdatenspeicherung mit einem Richter wisse DA, dass der juristische Bereich regelmäßig Probleme habe, Informationen wie eine Kfz-Zulassung oder einen Führerschein über Bundesländergrenzen hinweg auszutauschen, wenn dies bspw. für einen laufenden Prozess nötig sei. Dieses Bsp. zeige, wie schwer es trotz Vernetzung sei, auf bereits vorliegende Daten zugreifen zu können. Dem Missbrauchspotential erfasster Daten sei durchaus zuzustimmen, aktuell könne jedoch nicht von einer Zweckentfremdung solcher Datenbestände ausgegangen werden.

NT: Tatsächlich gebe es in der Auswertung von Beweismitteln das Problem, bei der Bearbeitung am Umfang der Datenbestände zu scheitern. NT könne jedoch vom Fall eines Mandanten berichten, der eine problematische Jugendzeit gehabt habe. Da der Mandant nach einigen Jahren in einem sicherheitsrelevanten Bereich habe arbeiten wollen, ließ er sich aufgrund der bevorstehenden Überprüfungen Auskunft darüber geben, welche Daten über ihn beim Bundes- und den Landeskriminalämtern gespeichert seien. Der Umfang der über ihn gespeicherten Daten sei immens gewesen. Obgleich es sein könne, dass der Datenaustausch zwischen den Behörden aktuell nicht

97 https://de.wikipedia.org/wiki/Maut (zuletzt aufgerufen: 20. Sep. 2015).

funktioniere, sei es erschreckend gewesen zu sehen, wie die Speicherfrist für jede „Jugendsünde“ des Mandanten in der Gegenwart verlängert wurde, sei dieser später bspw. an einem Autounfall beteiligt gewesen. Daneben landeten Bürger_innen immer in polizeilichen Datenbanken, sollten diese im Zusammenhang einer strafbaren Handlung verdächtigt werden, an dieser beteiligt gewesen zu sein. Selbst nach positiver Aufklärung solcher Verdachtsmomente lösche die Polizei nie von sich aus entsprechende Einträge, vielmehr halte sie mit aller Macht einmal gesammelte Daten vor.

Mod. RH: Prof. Dr. Giessmann habe in der vergangenen Veranstaltung „Vom Sinn der Kryptographie“ die Forderung des ehem. Bundesinnenministers Manfred Kanther erwähnt, Kryptographie strikt zu regulieren, um Überwachung zu erleichtern.[98] Diese Forderung stehe im Zusammenhang mit der „Krypto-Regulierung“[99] aus dem Jahre 1997, die vor staatlichen Abhörmaßnahmen gesicherte Verbindungen in Deutschland unmöglich machen sollte. [an DA] Gebe es Bemühungen in der Tagespolitik für ein Recht der Bürger auf gesicherte Kommunikation, bspw. In Form eines „Grundrechts auf Kryptographie“?

DA: Zum Glück sei es aktuell möglich so viel und umfangreich zu verschlüsseln wie man dies wolle. Dennoch habe die damalige Debatte sehr deutlich gezeigt, wie eine Regulierung von Kryptographie aussehen würde, bspw. durch Vorgabe bestimmter Verfahren oder entsprechender Parameter, bspw. die Begrenzung von Schlüssellängen. Diese Debatte sei aber in der politischen Diskussion aktuell nicht mehr zu finden. Parallel ereigneten sich aber alternative Versuche, Kryptographie zu unterwandern. Die NSA habe versucht, bei der US-amerikanischen Standardisierungsbehöre NIST[100] Verschlüsselungsmethoden als sicher einstufen zu lassen, deren Unsicherheit durch Kryptolog_innen bereits nachgewiesen worden sei. Das hier angesprochene, vom NIST zertifizierte Verschlüsselungsverfahren werde sehr häufig eingesetzt, um sichere Zugänge zu Firmennetzwerken großer Unternehmen herzustellen, wie DA aus persönlicher Erfahrung bestätigen könne. Daraus werde deutlich, wie Geheimdienste fernab staatlicher Gesetzesinitiativen Behörden missbrauchten, um sich langfristig Zugänge in geschlossene Netzwerke zu sichern. Aus Deutschland sei DA ein vergleichbarer Fall noch nicht bekannt. In diesem Zusammenhang spiele jedoch auch der Umstand eine bedeutende Rolle, dass die in Europa verwendete Kommunikationstechnologie nicht aus Europa stamme. Dies betreffe die Herstellung von Computerchips, Algorithmen sowie Standardisierungs- und Zertifizierungsmethoden. So werde auf eine Kommunikationstechnik vertraut, deren Sicherheit schwer nachgeprüft werden könne. Dies sei eine industriepolitisch interessante Problematik.

Daneben gebe es durchaus Versuche, Verschlüsselungstechnik für Normalnutzer_innen zu vereinfachen, wie die finanzielle Initiative für das Verschlüsselungspaket „Gpg4win“ des Bundesamtes für Sicherheit in der Informationstechnik gezeigt habe.[101] Initiativen wie diese hätten das Potential,

98 S. „Offene Diskussionsrunde der Gastvorträge“ im Protokoll zur Veranstaltung „Vom Sinn der Kryptographie“.

99 Vgl. KOSSEL, A.: „Datenschutz ade – Kanther fordert Krypto-Gesetz“, ct 6/97, online abrufbar unter: http://www.heise.de/ct/artikel/Datenschutz-ade-285626.html – Kurzlink: http://kurzlink.de/0XVGVEghT (zuletzt aufgerufen: 28. Aug. 2015).

100 https://de.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology (zuletzt aufgerufen: 28. Aug. 2015).

101 „Gpg4win – Sichere E-Mail- und Datei-Verschlüsselung“, bsi.bund.de, online abrufbar unter: https://www.bsi.bund.de/DE/Themen/ProdukteTools/Gpg4win/gpg4win_node.html – Kurzlink: http://kurzlink.de/HXEsQHHfK (zuletzt aufgerufen: 28. Aug. 2015).

nachhaltig etwas für den Datenschutz zu bewirken. So gebe es aktuell eine Förderung des Bundesministeriums für Bildung und Forschung (BMBF)[102] für Forschungsinitiativen zur Verbesserung des Datenschutzes für den Privatbereich.[103] Projekte und Initiativen wie diese förderten industriepolitische Autonomie.

Mod. AC: Die Ausführungen zeigten ein Bild, in welchem der deutsche Staat sich durchaus darum bemühe, seine Bürger_innen vor Überwachung zu schützen. Könne in diesem Zusammenhang tatsächlich von einem gesamtpolitischen Bemühen gesprochen werden? Schließlich zeige doch die aktuelle Debatte den vielfachen Austausch von gesammelten Überwachungsdaten zwischen westlichen Geheimdiensten.[104]

DA: [an Mod. AC] DA könne nicht für die Bundesregierung sprechen, aber sie habe die Vermutung, die Problematik um die Überwachungsaffäre sei nicht vollumfänglich in den hohen Kreisen der Politik angekommen. Aus persönlichem Umgang mit höheren Politiker_innen sei ihr deutlich geworden, dass diesen in den üblichen tagespolitischen Themen im Gegensatz zur Überwachungsaffäre die jeweilige Problematik bekannt und verständlich sei, sie entsprechende Lösungsvorschläge parat hätten und die Themen von der Presse wesentlich lieber wahrgenommen würden. Diese Faktoren allein zeigten schon, warum es aus Sicht besagter Politiker_innen leider als sinnvoller empfunden werde, sich um die vielfachen tagespolitischen Probleme außerhalb der Überwachungsaffäre zu kümmern. Die als abstrus empfundene Spionageaffäre sei ein unbeliebtes Terrain. Hier fehle es an Druck aus der Wirtschaft und vor allem aus der Bevölkerung. Dies läge vor allem an aktuell mangelnder persönlicher Betroffenheit. Druck aus Wirtschaft und Bevölkerung erzeuge medialen Druck, durch den das Thema politische Bedeutung bekomme. Es sei nun wichtig, für den Moment der politischen Beachtung des Themas, Ideen für die Selbstschutzmöglichkeiten der Bevölkerung zu liefern.

NT: [an Mod. AC] Die Politik spreche durchaus von einer Notwendigkeit des Schutzes der Bevölkerung vor Datenmissbrauch durch Unternehmen. Die Notwendigkeit für eine sichere Kommunikation im virtuellen Raum werde also gesehen. Komme die Politik aber zu Themen wie Strafverfolgung, Terrorismusbekämpfung und Kinderpornographie, seien Hintertüren in abgesicherter Kommunikation eine selbstverständliche Forderung.

Mod. RH: [an DrAK] Die letzte Synode der Evangelischen Kirche in Deutschland (EKD) habe unter dem Motto „Kommunikation des Evangeliums in der digitalen Gesellschaft“ gestanden.[105] Die Verlautbarungen dieser Synode seien in Bezug auf die Enthüllungen Edward Snowdens und zur Person Edward Snowden selbst recht verhalten gewesen. Das Lesebuch der Synode erwähne auf ca. 150 Seiten den Namen „Edward Snowden“ in lediglich drei Beiträgen, nur ein einziger davon sei ein

102 http://www.bmbf.de/ (zuletzt aufgerufen: 20. Sep. 2015).

103 »Bekanntmachung des Bundesministeriums für Bildung und Forschung von Richtlinien zur Förderung von Forschungsinitiativen auf dem Gebiet des Selbstdatenschutzes im Rahmen des Förderprogramms „IKT 2020 – Forschung für Innovationen“«, bmbf.de, 13. Okt. 2014, online abrufbar unter: http://www.bmbf.de/foerderungen/25038.php (zuletzt aufgerufen: 28. Aug. 2015).

104 Anm. d. Pr.: Vgl. „Verfassungsschutz weitet Zusammenarbeit mit US-Geheimdiensten aus“, sueddeutsche.de, 11. Jun. 2014, online abrufbar unter: http://www.sueddeutsche.de/politik/spionage-verfassungsschutz-weitet-zusammenarbeit-mit-us-geheimdiensten-aus-1.1995426 – Kurzlink: http://kurzlink.de/HDcjpmdKj (zuletzt aufgerufen: 28. Aug. 2015).

105 Vgl. »Lesebuch zur Vorbereitung auf das Scherpunktthema „Kommunikation des Evangeliums in der digitalen Gesellschaft“«, ekd.de, online abrufbar unter: http://www.ekd.de/synode2014/schwerpunktthema/lesebuch/index.html (zuletzt aufgerufen: 30. Aug. 2015).

theologischer und stamme von DrAK selbst. Es stelle sich die Frage, welche Ursachen diese Zurückhaltung habe. Im eingangs erwähnte Deutschlandfunk-Beitrag, in welchem Überwachung mit einer viralen Infektion verglichen werde, komme der Autor Friedemann Karig zu folgender Feststellung: „Dazu waren wir Menschen immer schon ein wenig einsehbar, sind Überwachung und Kontrolle gewöhnt. Ihre Geschichte reicht weit zurück: vom allsehenden, strafenden Gott über seine irdische Überwachungstechnik der Beichte bis hin zu Gesundheitsdaten auf Chipkarten.“[106] Der Vertreter des „Neuen Atheismus“, Richard Dawkins, erwähne in seinem Buch „Der Gotteswahn“ den „verstohlenen Blick [Anm. d. Pr.: des religiösen Menschen] zur großen Überwachungskamera im Himmel“, wobei er den Gottesgedanken auch als eine „kleine Abhörwanze [Anm. d. Pr.: im] Kopf“ bezeichne.[107] Lebe demnach „der Christ“ in einer Art Überwachungstradition, aus der heraus sich auch die Zurückhaltung gegenüber Edward Snowden auf der EKD-Synode erklären ließe?

[Zuspruch aus der Hörer_innenschaft]

DrAK: Es sei in der Tat etwas bedauerlich, dass sich die Evangelische Kirche bezüglich Edward Snowden und seiner Enthüllungen recht bedeckt halte. Das Ergebnis dieser/der Synode sei in einer Kundgebung verschriftlicht worden, die zur Überwachungsaffäre zumindest folgendes meine: „Wir erinnern den Staat an seine Verpflichtung, die Grundrechte seiner Bürgerinnen und Bürger zu sichern. Angesichts des fortwährenden Verstoßes gegen die Grundrechte im Bereich digitaler Daten fordern wir die Bundesrepublik Deutschland und die Europäische Union auf, für eine digitale Infrastruktur zu sorgen, die nicht nur technisch, sondern auch grundrechtssichernd funktioniert.“[108] Obgleich sich aus dieser Formulierung Verknüpfungen zur Tradition der Bekennenden Kirche herstellen ließen, welche sich zur Zeit der Nazi-Diktatur mit den Thesen der sog. „Barmer Theologischen Erklärung“ gegen die Nazi-Herrschaft bekannte, sei die aktuelle Zurückhaltung der EKD in Anbetracht der Umfänglichkeit globaler Überwachung zu groß.[109] DrAKs These nach sei es ein genuin protestantisches Thema, Gewissens- und Gedankenfreiheit nachdrücklich einzufordern. In der Vielfalt theologischer Themen sollte die Evangelische Kirche sich dieses, ihr eigenes Thema, folglich auch zu eigen machen.

Bezüglich der Idee, auf Gott als den „ewigen Abhörer“ die aktuell scheinbare Unempfindlichkeit von Christ_innen gegen Überwachung zurückzuführen, bestehe der Clou gerade in der Tatsache, dass Gott derjenige sei, der alles sehe und höre, wie es schon in alttestamentlichen Psalmen zum Ausdruck gebracht werde.[110] In diesen Texten bestehe die Gottesbeziehung jedoch aus vertrauensvoller Hingabe, bei der das religiöse Individuum nichts verheimlichen müsse, weil es sich der Allwissenheit und der

106 KARIG, F.: „Staatliche Überwachung - Befallen vom Überwachungsvirus“, deutschlandfunk.de, 04. Jan. 2015, online abrufbar unter: http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639 – Kurzlink: http://kurzlink.de/zasSFYovB (zuletzt aufgerufen: 30. Aug. 2015).

107 DAWKINS, R.: „Der Gotteswahn“, Berlin, 6 2007, 315.

108 SCHWAETZER, I.: „Kundgebung: Kommunikation des Evangeliums in der digitalen Gesellschaft“, ekd.de, 12. Nov. 2014, online abrufbar unter: https://www.ekd.de/synode2014/schwerpunktthema/beschluss_kundgebung.html (zuletzt aufgerufen: 30. Aug. 2015).

109 „Barmer Theologische Erklärung“, ekd.de, online abrufbar unter: http://www.ekd.de/glauben/bekenntnisse/barmer_theologische_erklaerung.html (zuletzt aufgerufen: 30. Aug. 2015).

110 Anm. d. Pr.: Vgl. bspw. Ps 139, online abrufbar unter: https://www.die-bibel.de/online-bibeln/luther-bibel-1984/bibeltext/bibelstelle/Ps%20139/bibel/text/lesen/ch/f62983854d8ba0e1d35d69af3c150823/#top – Kurzlink: http://kurzlink.de/Mlb8YPmLZ (zuletzt aufgerufen: 30. Aug. 2015).

Güte Gottes bewusst sei. Aktuell sei es jedoch so, dass sich Geheimdienste für ihr Ziel einer Allwissenheit über sämtliche Geschehnisse in der Welt zu Göttern aufspielten und deren Verantwortliche sich demzufolge eine autoritäre Macht anmaßten, die ihnen nicht zustehe. Daher sei Überwachung auch ein theologisches Problem, aus welchem sich die Forderung ableite, der Überwachung Einhalt zu gebieten. Der beschriebene Zustand, nach welchem sich amerikanische wie deutsche „Geschöpfe“ mit dem „Schöpfer“ verwechselten, müsse der Kirche viel deutlicher werden, da in dieser Verwechslung eine große Sünde stecke.

[Zuspruch aus der Hörer_innenschaft]

Mod. RH: Die letzte Frage beziehe sich auf die Problematik des Asyls für Edward Snowden in Deutschland, die in den Verlautbarungen der angesprochenen EKD-Synode mit keinem Wort thematisiert wurde. Edward Snowden sei die Möglichkeit zu verdanken, die aktuelle Debatte in dieser Form weltweit führen zu können. Zugleich sei Edward Snowden aber ausgerechnet in demjenigen Land Asyl gewährt worden, dem ein der westlichen Welt vergleichbares Niveau an Rechtsstaatlichkeit oftmals abgesprochen werde. RH vermisse daher auch eine Forderung der Kirchen, Edward Snowden Asyl in Deutschland zu gewähren. [An DA, DrAK und NT] Sei die Forderung „Asyl für Snowden in Deutschland“ eine moralische Pflicht oder lediglich ein willkommenes Argument der jew. politischen Opposition?

DA: Der Forderung „Asyl für Snowden“ werde persönlich absolut zugestimmt. Besonders für die zukünftige Aufklärungsarbeit durch Edward Snowden sei der Umstand, in Russland festzusitzen, schwierig, da Snowden dort sicher nicht alles äußern könne, was er wolle.[111] Die Situation sei daher im aktuellen Zustand für ihn sehr belastend. Aus idealistischer Sicht spreche sich DA daher klar für ein Asyl Snowdens in Deutschland aus. Realistisch betrachtet sei jedoch sehr zu befürchten, dass eine Einreise Snowdens in Deutschland eine sofortige Auslieferung Snowdens an die Vereinigten Staaten von Amerika nach sich ziehe. Die Bundesregierung habe diesbezüglich deutlich gemacht, kein Risiko für ihre internationalen Beziehungen eingehen zu wollen und daher Snowden weder in den NSA-Untersuchungsausschuss einzuladen, noch ihm Asyl zu gewähren. In Bezug auf den NSA-Untersuchungsausschuss sei es unverständlich, warum Edward Snowden als der Hauptzeuge der Angelegenheit nicht eingeladen werde. Zugleich dürfe jedoch nicht der Fehler begangen werden, die Überwachungsproblematik lediglich auf die Person Edward Snowden zu beschränken, wie dies in den Medien aktuell der Fall sei. Demnach sei die Forderung „Asyl für Snowden“ eine legitime und unterstützenswerte, die allerdings auch leicht die eigentliche Problematik um die Überwachung durch Geheimdienste aus dem Fokus dränge.

Hörer_in: Einwurf der These, die Bundesregierung könne Snowden durchaus Asyl gewähren und eine Auslieferung Snowdens verhindern.

Mod. RH: [an Vorredner_in] Bitte, den Einwand noch einmal in der offenen Diskussion einzubringen.

111 Anm. d. Pr.: Vgl. die 2013 von Vladimir Putin geäußerte Bedingung zum Bleiberecht Snowdens: „If he wants to go somewhere and someone will take him, go ahead. If he wants to stay here, there is one condition: he must stop his work aimed at harming our American partners, as strange as that sounds coming from my lips.“ [„Wenn er irgendwo anders hin gehen und ihn jemand aufnehmen möchte, so steht ihm dies frei. Möchte er hier bleiben, gibt es eine Bedingung: Er muss seine Anstrengungen einstellen, die dagegen gerichtet sind, unseren amerikansichen Partnern zu schaden, so seltsam sich dies aus meinem Mund auch anhören mag.“], in: „News conference following the working meeting of the Gas Exporting Countries Forum (GECF) summit“, kremlin.ru, 01. Jul. 2013, online abrufbar unter: http://en.kremlin.ru/events/president/transcripts/18441 (zuletzt aufgerufen: 03. Sep. 2015).

DrAK: Hätte Martin Luther nicht unter dem Schutz des Kurfürsten Friedrich III. gestanden, der ihm Zuflucht auf der Wartburg ermöglichte, wäre Luther sicher der über ihn verhängten Reichsacht zum Opfer gefallen. Ein entsprechender Schutz sei Edward Snowden ebenso zu gönnen.[112]

NT: Die Gefahr einer Auslieferung, sobald Edward Snowden deutsches Staatsgebiet betrete, sei überaus hoch. Es sei daher sehr wünschenswert, Snowden Asyl zu gewähren.

DA: Der Zwischenfall der erzwungenen Landung der bolivianischen Präsidentenmaschine verdeutliche die Schwierigkeiten, die der Versuch Snowdens nach sich ziehe, die Russische Föderation zu verlassen. Das Flugzeug des bolivianischen Präsidenten Evo Morales sei im Juli 2013 auf den Verdacht hin, auf einer Abreise aus Moskau Edward Snowden heimlich nach Südamerika auszufliegen, in Wien zur Landung gezwungen worden.[113]

NT: Dieser Zwischenfall sei ein Armutszeugnis.

DA: Dieses Armutszeugnis sei Realität.

Mod. RH: Das Armutszeugnis ziele vielleicht auf einen philosophischen, von John Locke im zuvor erwähnten Beitrag des Deutschlandfunks zitierten Gedanken ab, der zum Verständnis des Begriffes „Staat“ folgendes sage: „Der Staat dient uns. Er ist ein Vertrag mit uns selbst, dessen Inhalte wir bestimmen. Verstößt er dagegen, müssen wir ihn zügeln.“[114]

Mit diesem Gedanken sei die Pause eröffnet, auf welche die offene Diskussion folge.

Offene Diskussion

Nach einer zehnminütigen Pause erfolgte die offene Diskussion zwischen Hörer_innenschaft und Podiumsgästen.

Mod. RH: [an DA] Als Informatikerin habe sich DA sicher auch mit dem Bereich der Kybernetik auseinandergesetzt. Der Begriff der Kybernetik leite sich aus dem altgr. Wort für „Steuermann“ ab und sei nicht nur eine Beschreibung für ein technisches, sondern auch ein theologisches Fachgebiet.[115] Im Zusammenhang mit dem Bereich der Kybernetik sei interessant, dass Facebook mit seiner Nutzer_innenschaft unbemerkt ein Experiment durchführte, um zu untersuchen, wie sich durch gezielte Platzierung von Informationen Nutzer_innen psychologisch beeinflussen ließen.[116] Zu diesem Zweck sei Facebook-Nutzer_innen gezielt Informationen in ihr persönliches Profil (Timeline) eingespielt bzw. Informationen, die andere Nutzer_innen mit ihnen teilten, ihnen unbemerkt vorenthalten worden. Dieses groß angelegte Experiment sei ein dunkles Einsatzszenario der Kybernetik, mittels der Auswertung

112 Anm. d. Pr.: Vgl. PRIEBE, M.: „Ist Snowden der moderne Luther?“, evangelisch.de, 16. Aug. 2013, online abrufbar unter: https://www.evangelisch.de/inhalte/87444/16-08-2013/ist-snowden-der-moderne-luther – Kurzlink: http://kurzlink.de/kP1T6Kk1c (zuletzt aufgerufen: 03. Sep. 2015).

113 Anm. d. Pr.: Vgl. MORALES, E.: „Brief aus der Luft“, monde-diplomatique.de, 09. Aug. 2013, online abrufbar unter: http://www.monde-diplomatique.de/pm/2013/08/09.mondeText1.artikel,a0012.idx,3 – Kurzlink: http://kurzlink.de/7WhUQnG8C (zuletzt aufgerufen: 04. Sep. 2015).

114 KARIG, F.: „Staatliche Überwachung - Befallen vom Überwachungsvirus“, deutschlandfunk.de, 04. Jan. 2015, online abrufbar unter: http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639 – Kurzlink: http://kurzlink.de/zasSFYovB (zuletzt aufgerufen: 04. Sep. 2015).

115 https://de.wikipedia.org/wiki/Kybernetik (zuletzt aufgerufen: 04. Sep. 2015).

116 BOOTH, R.: „Facebook reveals news feed experiment to control emotions“, theguardian.com, 30. Jun. 2014, http://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds (zuletzt aufgerufen: 04. Sep. 2015).

großer Datenmengen Nutzer_innen unbewusst zu steuern.[117] Wie plausibel sei demnach das Szenario einer bewussten Steuerung von Bürger_innen außerhalb des virtuellen Raumes?

DA: Von der beschrieben Steuerung sei ohne Frage auszugehen und eine Meinungssteuerung der Bevölkerung nichts Neues. Fraglich sei, wie strukturiert eine solche Steuerung stattfinde. Die Presse sei in diesem Zusammenhang eine Säule des politischen Systems, die sowohl in Richtung Bevölkerung als auch Politik eine Steuerungsfunktion übernehme. Manipulation der Rezipient_innen fände vor allem aus marktwirtschaftlichem Interesse bei Boulevardmagazinen statt. Eine staatlich organisierten Steuerung und Manipulation der Bevölkerung sei jedoch schwer vorstellbar, da der innenpolitische Alltag für ein solches Unterfangen von DA als zu chaotisch empfunden werde.

Daneben könne jede(r) Nutzer_in feststellen, in einer Art individuellen Informationsblase („Filterbubble“) gefangen zu sein, die durch die eigenen, zwischenmenschlichen Kontakte geprägt sei und einen Spiegel der eigenen Meinung darstelle.[118] Die Suche von Begriffen im Internet führe in diesem Zusammenhang dazu, dass die für die Suchfunktion zuständigen Algorithmen der Internetdienste Nutzer_innen in bestimmte Nutzergruppen kategorisierten. Derartige Kategorisierungsalgorithmen der Art „Hausfrau, vierzig Jahre, zwei Kinder“ verstärkten den Effekt der individuellen Informationsblase durch maßgeschneiderte Unterbreitung von Internetinhalten. Zwar funktionierten derartige Algorithmen aktuell nur mit einer überschaubaren Trefferquote, da aktuell personalisierte Werbung zumindest bei DA den tatsächlichen Vorlieben kaum entspreche, aber die Algorithmen würden stetig verbessert werden. Die Gefahr bestehe weniger in einer Steuerung der Gesellschaft, sondern mehr in den Mechanismen, die Bürger_innen durch Kategorisierung in eine Art Korsett pressten, sodass diese mehr und mehr als Stereotypen und weniger als Individuen behandelt würden. Im Zusammenhang mit derartigen Kategorisierungsalgorithmen sei das Thema Big Data[119] ein wichtiges Schlagwort für statistische Algorithmen, mit denen sich aus bereits gesammelten Daten ein Maximum an Informationen herauslesen lasse. Aus der Gewinnmaximierung von gesammelten Daten mittels „Big Data“ bestehe das Geschäftsmodell von Unternehmen wie Facebook und Google. Ähnliche Verfahren würden auch von Geheimdiensten genutzt, um Verhaltensmuster von Nutzer_innen zu erstellen.

Die Gefahr bestehe demnach in einer Überkategorisierung der Bürger_innen, die ein besonderes Gefahrenpotential entfalte, sobald es zu einer positiv-negativ-Kategorisierung komme. Fehltritte des Individuums gegen gesellschaftliche Normen könnten in einer solchen Kategorisierung auch dazu führen, aus positiven Kategorien herauszufallen. Einstufungssysteme wie das der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) seien ein Bsp. für ein bereits weit verbreitetes gesellschaftliches Einstufungssystem mit tiefgreifenden Auswirkungen auf die Bürger_innen.

---

117 KARIG, F.: „Staatliche Überwachung - Befallen vom Überwachungsvirus“, deutschlandfunk.de, 04. Jan. 2015, online abrufbar unter: http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639 – Kurzlink: http://kurzlink.de/zasSFYovB (zuletzt aufgerufen: 30. Aug. 2015).

118 PARISER, E.: „Filter bubble : wie wir im Internet entmündigt werden / Eli Pariser. Aus dem Amerikan. von Ursula Held“; München, 2012, Katalog der Deutschen Nationalbibliothek: http://d-nb.info/1017530424 (zuletzt aufgerufen: 02. Okt. 2015).

119 https://de.wikipedia.org/wiki/Big_Data (zuletzt aufgerufen: 07. Sep. 2015).

Der kommerzielle Wert von Informationen und Daten sei zu vergleichen mit dem von Gold, sodass sowohl Unternehmen als auch Staaten ein umfangreiches Interesse an der Anhäufung ihrer Datenbestände hätten. Die Politik wisse um den Wert derartiger Datenbestände, da sich mit genauen Informationen über die Bevölkerung bspw. ein Wahlkampf bis in einzelne Straßenzüge hinein so individualisieren ließe, dass ein Popularitätsgewinn für die jew. Partei garantiert sei. Unter dem Ideal einer Demokratie aus Individuen, die diese ausgestalteten, stimme eine solche Zukunftsaussicht pessimistisch.

Hörer_in: [an DrAK] In Deutschland zeichne sich eine tiefgreifende Islamfeindlichkeit ab. Umfragen hätten gezeigt, dass ein Großteil der deutschen Bevölkerung den Islam für eine gewaltbereite Religion halte, die sich bspw. in der PEGIDA-Bewegung äußere. Im Zusammenhang mit den Anschlägen auf das Redaktionsbüro von Charlie Hebdo in Paris forderten vor allem christliche Parteien eine Rückkehr zur Vorratsdatenspeicherung. Sei die Rolle der Kirchen in Anbetracht der offensichtlichen Handlungsunfähigkeit politischer Parteien auch darin zu sehen, Vertrauen sowie ein neues Selbstverständnis in der Basis der Bevölkerung zu schaffen, sich bspw. im Sinne des zuvor erwähnten Philosophen John Locke und abseits von politischen Parteien selbst als den Staat zu verstehen und als solcher zu agieren?

DrAK: [an Vorredner_in] Die evang. Kirche sei eine von mehreren entscheidenden Größen in der deutschen Gesellschaft und präge entsprechend die Bürger_innen, aus denen schließlich Entscheidungsträger_innen der Gesellschaft hervorgingen. Entsprechend habe sie den Auftrag, ein verantwortungsvolles Selbstverständnis der Menschen mit zu prägen. Diesem Auftrag werde sie nicht immer gerecht, es sei daher wünschenswert, besonders auch in Bezug auf das Thema Vertrauen für eine Freiheit des Austausches von Gedanken einzutreten, da nur durch den Schutz der Gedankenfreiheit eine Demokratie am Leben erhalten werden könne. Ein freiheitlicher Gedankenaustausch, der die gefahrlose Teilhabe der Mitmenschen an den eigenen Gedanken ermögliche, bewirke schließlich erst, Vertrauen zwischen den Menschen entstehen zu lassen. Ein beständiges Verdächtigen in Kommunikationsprozessen wirke genau entgegengesetzt.

Hörer_in: Die Reaktion der die Bürger_innen vertretenden Parteien sei erstens durch den/die Hörer_in als sehr kleinlaut empfunden worden. Für die etablierten Parteien gebe es zweitens keinen Grund, an den Überwachungspraktiken etwas zu ändern. Vor allem die Regierungsparteien hätten das Problem der Rechtfertigung gegenüber der Bevölkerung, im Bereich der Sicherheitspolitik und Gefahrenabwehr alles für den Bevölkerungsschutz getan zu haben. Drittens sei zu bedenken, dass alle Parteien aktueller und vergangener Legislaturperioden in einer Mitverantwortung für die Überwachungsaffäre stünden. Zwar seien die deutschen Parteien nicht mehr als Leichtmatrosen im Boot der NSA, die nur an Bord säßen, weil sie geduldet würden, sie trügen dennoch eindeutig eine Mitschuld an der Überwachungssituation, da sie diese heimlich gedeckt hätten. Diese Mitschuld hindere Parteispitzen daran, sich offen gegen globale Überwachung auszusprechen.[120] Die Frage sei nun, wie dieses Problem

120 Anm. d. Pr.: Vgl. „Land unter Kontrolle“, TV-Dokumentation, 3Sat/ZDF/zdf.info 2014, online abrufbar unter: http://www.candoberlin.de/filme/land-unter-kontrolle-lang/ (zuletzt aufgerufen: 10. Sep. 2015).

zu lösen sei. Wer vertrete die Interessen derer, die an diesem Abend hier zusammensäßen und Initiativen gegen Überwachung für gerecht und wesentlich hielten? Welche Stimme könne unterstützt werden, die hier diskutierten Anliegen zu vertreten?

DA: [an Vorredner_in] Erstens sei wichtig, in der Angelegenheit nicht zu resignieren. In diesem Zusammenhang bedeute die zuvor genannte These, Parteien seien nicht handlungsfähig, eine eigene Resignation vor den vorhandenen demokratischen Möglichkeiten. Engagement gegen Überwachung könne sehrwohl über Mitarbeit in Parteien funktionieren, obgleich Parteiarbeit überaus anstrengend sei, bedenke man die Schwierigkeiten, Themen wie die Überwachungsaffäre innerhalb einer Partei auf die Tagesordnung zu bringen. Dennoch sei es parteiübergreifend möglich, auf diese Weise gesamtgesellschaftliche Impulse zu liefern. In der Evangelischen Kirche bestünden ähnlich schwierige, dennoch ähnlich basisdemokratische Wege. Der von DrAK aus der EKD-Synode zitierte Abschnitt [Anm. d. Pr.: s.v. „Wir erinnern den Staat an seine Verpflichtung [...]“] sei ein Impuls, der bspw. im Vergleich zu den Inhalten, die in der Digitalen Agenda[121] der Bundesregierung zum Thema Überwachung formuliert worden seien, relativ viel Gehalt habe und relativ konkret sei. [Zuspruch aus der Hörer_innenschaft] Daher sei es ausgesprochen wichtig, seitens der Bevölkerungsbasis immer wieder auf Themen wie die Überwachungsaffäre aufmerksam und so diese zum Gegenstand der Tagespolitik zu machen. Die Legitimation dafür ziehe sich bspw. innerhalb der SPD aus den drei Grundwerten der Partei, von denen eine „Freiheit“ laute. Bürger_innen müssten entsprechend in ihrem jeweiligen Alltagsbereich ihren Mitmenschen verdeutlichen, sich gegen Überwachung zu engagieren. Dies könne in jeder Form von Organisation erfolgen. Die Organisationsform einer politischen Partei sei auf jeden Fall eine handlungsfähige, sofern man sich darüber im Klaren sei, dass Initiativen wie diejenigen gegen Überwachung keine „Zwei-Monats-Projekte“ seien, vor allem, wenn die Gegenfaktoren so stark ausgeprägt seien wie es aktuell der Fall sei.

Vorredner_in: [an DA] Einwurf der Frage, ob auf diesem Wegen nicht die Gefahr bestehe, den „Bock zum Gärtner“ zu machen.

DA: [an Vorreder_in] Die Überforderung eines erheblichen Teils der Bevölkerung, die mit dem Digitalen Wandel nicht aufgewachsen sei, dürfe nicht unterschätzt werden. Entsprechend sei klar, dass auch ein bedeutender Teil der älteren Politiker_innen mit einer digitalisierten Welt erst umzugehen lernen müsse. Gemessen am zeitlichen Umfang eines durchschnittlichen Abgeordnet_innentages sei es bereits erfreulich zu sehen, wenn Politiker_innen MacBooks oder iPads bedienen könnten.

Hörer_in: [an Vorredner_in] Einwurf der Frage, ob demnach Günther Oettinger[122] den richtigen Posten inne habe.

DA: [an Vorreder_in] Die Entscheidung zur Vergabe dieses Postens habe den Zweck einer „Parkposition“ gehabt.

[Zuspruch aus der Hörer_innenschaft]

121 http://www.bmwi.de/DE/Themen/Digitale-Welt/digitale-agenda.html (zuletzt aufgerufen: 10. Sep. 2015).

122 Anm. d. Pr.: Günther H. Oettinger ist EU-Kommissar für „Digitale Wirtschaft und Gesellschaft“, vgl. https://ec.europa.eu/commission/2014-2019/oettinger_de (zuletzt aufgerufen: 11. Sep. 2015).

NT: Bürger_innen könnten sich in der Überwachungsthematik nicht auf politische Parteien verlassen. Bürger_innen müssten dagegen individuell Initiative ergreifen, auch ohne sich dafür in Parteien organisieren zu müssen. Es gebe genügend Gruppierungen, die sich um Einzelbereiche wie den der Netzpolitik kümmerten. Die Zersplitterung bürgerlicher Initiativen sei dabei zwar ein Hindernis für das Ziel, sich auf möglichst breiter Ebene Gehör zu verschaffen, NT könne aber trotz dieser Zersplitterung in der Rezeption ihrer digitalen Informationskanäle durchaus viel Initiative und Bewegung gegen Überwachung erkennen. Wichtig sei, sich beständig zu informieren, aktiv zu werden und anzufangen, sich selbst im digitalen Raum zu schützen.

Hörer_in: [an Vorredner_in] Einwurf der These, dass die Entwicklung einer „gesunden Wut“ in der Liste wichtiger Maßnahmen bürgerlicher Initiative ebenso nötig sei.

NT: [an Vorredner_in] Wut sei in diesem Zusammenhang eine problematische Angelegenheit, allerdings seien Misstrauen und Unnachgiebigkeit angebracht.

Hörer_in: Es sei spürbar, dass die Überwachungsaffäre alle hier Anwesenden aufgewühlt habe. Die Enthüllungen von Edward Snowden seien unglaublich. Empörung und Ereiferung sei das Resultat. Eine alternative Herangehensweise, die Problematik zu lösen, bestehe eventuell darin, zunächst die globale Überwachung als gegeben zu akzeptieren, um schließlich nach Umgangsmöglichkeiten und Methoden bzw. Kompetenzen einer Gegensteuerung zu fragen. Das gesellschaftliche Problem der Politikverdrossenheit schließe die Möglichkeit einer basisgesellschaftlichen politischen Initiative aus. Es gäbe jedoch die Möglichkeit, durch digitale Medien Zivilcourage zu zeigen und Antworten auf die aktuellen Fragen zu geben statt an die politische Ebene Forderungen zu stellen. Dafür sei zunächst wichtig, festzustellen, welche offenen Fragen im Hinblick auf ein tiefes Verständnis der Überwachungsaffäre existierten. Verschlüsselung sei bspw. eine Kompetenz, die erstens mit hohen zu meisternden Hürden einhergehe und zweitens die Frage aufwerfe, wie weit es möglich und sinnvoll sei, gegen einen Geheimdienst wie den der NSA aufzurüsten. Die Frage sei also, welche Kompetenzen in der Zukunft benötigt würden, um mit den aktuellen gesellschaftlichen Veränderungen umgehen zu können.

Hörer_in: [an Vorredner_in] Einwurf der These, der Politik komme in jedem Fall eine entscheidende Rolle hinzu, da sie die gesetzgebende Instanz sei.

Hörer_in: [an Vorredner_in] Entgegnung, die Politik werde jedoch letztlich durch Wahlen bestimmt.

Hörer_in: [an Vorredner_in] Entgegnung, die Wahlbeteiligung sei diesbezüglich zu niedrig.

Hörer_in: Einwurf der These, die Politik entscheide bspw. darüber, dass den Schüler_innen ein Informatikunterricht auf lächerlichem Niveau erteilt werde. Aktuell seien Kompetenzen zur Überwachungsabwehr nur durch Eigeninitiative zu erwerben und liefere Menschen, welche die technischen Geräte nutzen könnten, aus, sich von diesen benutzen zu lassen. Desweiteren sei festzustellen, dass die aktuell heranwachsende Generation an Jugendlichen ein gänzlich anderes Verständnis von Datenschutz habe als bspw. diejenigen Bürger_innen, die es gegen Überwachung in BRD und DDR auf die Straßen getrieben habe. Ein solches Störempfinden sei von der aktuellen Generation an Jugendlichen nicht mehr zu erwarten. So müsse die Aufforderung an Bürger_innen und

Politik darin bestehen, junge Menschen für die Gefahren der Überwachung zu sensibilisieren, da sich diese elementar auf das Leben auswirke. Aktuell sei bspw. der Informatikunterricht in Berlin ein Alptraum und biete jungen Menschen in Bezug auf das gegenwärtige Überwachungsproblem rein gar nichts.

Hörer_in: [an Vorredner_in] Eltern müssten daher die Vermittlung von Kompetenzen zur Abwehr von Überwachung im Informatikunterricht einfordern.

Hörer_in: Gemessen an der politischen Bedeutung, die der Bildung über die sich wiederholenden Diskussionen zur Frage einer angemessenen Gymnasialzeit beigemessen werde, sei es an der Zeit, die Inhalte der Schulbildung den Umständen entsprechend förderlicher zu definieren.

NT: [an Vorredner_innen] Das Probleme lasse sich nicht allein durch Bildung der Schüler_innen lösen. Bürger_innen fernab der Schule seien ebenso schutzlos der Überwachung ausgeliefert und müssten entsprechende Fortbildungsmaßnahmen erhalten. NT wisse von Deutschlehrer_innen, die als Teil des Lehrplanes auch das Schreiben von E-Mails behandelten, diesbezüglich aber aufgrund mangelnden Hintergrundwissens keinerlei Bezug auf die Datenschutzproblematik nehmen könnten, die in diesem Zusammenhang unbedingt vermittelt werden müsse. Vermittlung von auf Datenschutz ausgerichtetem Wissen müsse daher generationenübergreifend vermittelt werden.

Für die angesprochene, gewünschte Empörung innerhalb der Bevölkerung sei wichtig zu verstehen, wie sehr sich aktuelle Überwachung von jener der Vergangenheit durch die nun technisch mögliche Unsichtbarkeit der Überwachungsmechanismen unterscheide.[123]

Hörer_in: [an NT] Einwurf der These, die Diskussion erinnere an diejenige der achtziger Jahre. Damals habe man sich mit der Tatsache abgefunden, überwacht zu werden, da es unmöglich sei, sich der Überwachung zu entziehen. Man habe jedoch zugleich entschlossen, sich deswegen nicht in der Meinungsfreiheit einschränken oder von „Paranoia“ unterkriegen zu lassen. Auf einem derartigen Entschluss müsse der Fokus aktuell ebenfalls liegen.

NT: [an Vorredner_in] Entgegnung, das Anliegen der Aussage NTs habe darin bestanden, die ausbleibende Empörung innerhalb der Bevölkerung mit der vorherrschenden Meinung der Bürger_innen zu erklären, dass es zwar eine Überwachung gäbe, diese aber das jeweilige Individuum nicht betreffe. Eine individuelle Betroffenheit durch Überwachung könne aktuell nicht eingeschätzt werden, was in der Bevölkerung dazu führe, eine persönliche Betroffenheit gänzlich abzustreiten, obgleich aufgrund der ungeklärten Situation die persönliche Betroffenheit alles andere als ausgeschlossen werden könne.

Hörer_in: [an NT] Entgegnung, das Anliegen der These habe nicht in einer Ablehnung einer persönlichen Betroffenheit bestanden, sondern in der Einschätzung, gegen Überwachung nichts ausrichten zu können.

NT: [an Vorredner_in] Entgegnung, die Teilnahme an dieser Veranstaltung zeige deutlich das Anliegen, sich aktiv gegen Überwachung wehren zu wollen.

123 Anm. d. Pr.: Vgl. „Über Umwege ans Ziel“, in: c't Magazin für Computertechnik 19/2015, 66, online abrufbar unter: http://www.heise.de/ct/ausgabe/2015-19-Lexikon-des-NSA-Skandals-Fashioncleft-2783647.html#1441243622005070_1439803924 – Kurzlink: http://heise.de/-2783647 (zuletzt aufgerufen: 16. Sep. 2015).

Hörer_in: [an NT] Entgegnung, die erwähnten Exkurse zur Überwachung in der Geschichte der Menschheit hätten verdeutlicht, wie bedeutend das Sammeln von Informationen zu allen Zeiten gewesen sei. Damit gehöre Spionage zur Geschichte der Menschheit und könne im digitalen Zeitalter erst recht kaum unterbunden werden.

Hörer_in: [an Vorredner_in] Einwurf der These, dass der angesprochene Vergleich zwischen analogem und digitalem Zeitalter nicht stimme. So sei bspw. der Aufwand zur Überwachung des Postverkehrs immens gewesen, weswegen bspw. das Ministerium für Staatssicherheit zweihunderttausend Mitarbeiter benötigt hätte. Aktuell jedoch sei das Volumen der zu überwachenden Kommunikation nicht mehr begrenzt, woraus sich eine neue Qualität der Überwachung ergebe. Daher müsse in der Geschichte der Überwachung nicht nur eine Linearität, sondern ein Sprung in eine völlig neue Dimension an Möglichkeiten von Überwachung gesehen werden. Konnten früher lediglich gezielt Einzelpersonen überwacht werden, sei es heute kein Problem, Bevölkerungen vollumfänglich überwachungstechnisch zu erfassen. Die persönliche Courage gegen Überwachung zu bewahren sei ein wichtiger Punkt, dennoch müsse vom Staat konsequent ein Ende der Massenhaftigkeit und Totalität der Überwachung eingefordert werden.

Hörer_in: [an Vorredner_in] Einwurf der These, die DDR habe in ähnlichem Ausmaß überwacht wie es aktuell der Fall sei.

Hörer_in: [an Vorredner_in] Entgegnung, in der DDR sei bspw. nicht der Schlafrhythmus über Smartphone-Applikationen erfasst worden. Es gehe in der Debatte nicht nur um Kommunikationsüberwachung, sondern um die Erfassung vielfacher Bereiche wie bspw. Steuerdaten, Krankendaten oder Maut-Daten, welche die vollständige digitale Darstellung eines Menschen zum Ziel habe.

Hörer_in: [beim Verlassen des Hörsaals] Einwurf der These, es sei ein Märchen anzunehmen, Politik meine es gut mit den Menschen. Von dieser Annahme müsse man sich trennen.

[Gelächter unter den Anwesenden]

Mod. RH: DA habe sich vielfach gemeldet, daher Übergabe des Wortes an DA.

DA: Die aktuelle Diskussion sei löblich. Frage an die Hörer_innenschaft für weitere Beiträge.

Hörer_in: Die Menge an über harmlose Normalbürger_innen gespeicherten Daten verwundere im Zusammenhang der weltweit unkontrolliert agierenden Kriminalität immer wieder. Aus Sicht von Normalbürger_innen sei es unverständlich, dass ein vorhandenes globales Überwachungssystem nicht in der Lage sei, Verbrechen zu verhindern, dennoch aber völlig uninteressante Handlungen von Bürger_innen erfasse.

Mod. AC: [an Vorredner_in] Entgegnung, es könne kaum eingeschätzt werden, ob diese erfassten Handlungen tatsächlich uninteressant seien. Die Unkenntnis darüber, für welchen Zweck die Überwachungssysteme Daten erfassten, sei das Problem. Die Ergreifung der Sauerland-Gruppe werde

oft als Bsp. für den gesellschaftlichen Mehrwert von Überwachung angeführt.[124] Es bestehe jedoch der Verdacht, dass mehr hinter den Überwachungssystemen stecke. Worin dieses „mehr“ bestehe, werde kaum erfragt.

Hörer_in: [an Vorredner_in] Entgegnung mit der These, die organisierte Kriminalität agiere wohl clever an den Überwachungssystemen vorbei. Es sei unbegreiflich, wie es trotz unvorstellbar umfassender Überwachung überhaupt zu umfangreichen Verbrechen kommen könne. Es stelle sich unter der angesprochenen These einer Digitalisierung aller Handlungen der Menschen die Frage, ob die globale Überwachung nicht eine Farce sei.

Mod. AC: Zum Abschluss der offenen Podiumsdiskussion müssten die folgenden Fragen gesammelt erfolgen.

Hörer_in: Es müsse eine Lanze für die Politik gebrochen werden. Zunächst sei festzustellen, dass es aktuell überhaupt nicht mehr möglich sei, der Erfassung eigener Informationen zu entgehen. Auch wenn man sich bspw. aktueller Smartphone-Technik verweigere, gelangten die eigenen Informationen dennoch in den Datenbestand von Überwachungssystemen, da bspw. beim Versand einer E-Mail selbst datenschutzbewusste Nutzer_innen ihre Daten über Umwege in Systeme wie Google Mail einspeisten, die sie selbst niemals benutzen würden. Der Vertrag, den Nutzer_innen bspw. mit Google Mail eingingen, gelte bei genauer Betrachtung nicht nur für die primären Vertragspartner_innen, sondern zwangsläufig für alle Mitmenschen, die mit diesen Google Mail-Nutzer_innen in Kontakt stünden. Es gehe folglich in der Überwachungsdebatte nicht um das Verhältnis zwischen Individuum und Unternehmen bzw. Staat, sondern um gesellschaftliche Effekte, die das Individuum unmöglich selbst lösen könne. Gesellschaftliche Probleme wie bspw. auch umweltpolitische Fragen könne allein die Politik lösen. Zwar sei Politikverdrossenheit aufgrund der sich häufig ins Gegenteil verkehrenden Wahlversprechen nachvollziehbar, allerdings müsse an dieser Stelle zugunsten der Politik zwischen Politikverdrossenheit und Parteienverdrossenheit unterschieden werden. Die Entwicklungen um den NSA-Untersuchungsausschuss zeigten leider, wie wirkungslos die Arbeit der Politik aktuell sei, wenn der BND zeitgleich zur Aufklärung eines Überwachungsskandals Millionen zur Entschlüsselung verschlüsselter Kommunikation investieren wolle.[125] Es dränge sich daher der Gedanke auf, dass die Überwachung nicht der Abwehr äußerer Feinde diene.

Mod. RH: Aufruf der nächsten Frage.

Hörer_in: Die Frage, warum eine Eindämmung der Kriminalität trotz Überwachung ausbleibe, basiere auf einer grundsätzlich falschen Denkweise. Mit dem Konzept der Verbrechensabwehr seien in der Vergangenheit immer Überwachungsstrategien und Aufrüstung des Sicherheitsapparates verkauft

---

124 Anm. d. Pr.: Vgl. GERHARDT, P., SENYURT, A.: „Terroristenjagd im Sauerland. Wie das BKA ein Blutbad verhinderte“, TV-Dokumentation, ARD 2009, Produktionsinformationen unter: http://www.deutsche-kinemathek.de/archive/fernseharchiv/T (zuletzt aufgerufen: 17. Sep. 2015);
Vgl. daneben VAN ROSSUM, W.: „Ein Käfig voller Enten?“, deutschlandfunk.de, 12. Mai 2009, online abrufbar unter: http://www.deutschlandfunk.de/ein-kaefig-voller-enten.1247.de.html?dram:article_id=190154 – Kurzlink: http://kurzlink.de/g4tKakEXS (zuletzt aufgerufen: 17. Sep. 2015).

125 Vgl. Beuth, P. „Wie der BND Verschlüsselung knacken will“, zeit.de, 14. Nov. 2014, online abrufbar unter: http://www.zeit.de/digital/datenschutz/2014-11/bnd-chipanalyse-triphemos-verschluesselung-knacken – Kurzlink: http://kurzlink.de/1hi3FAEzj (zuletzt aufgerufen: 17. Sep. 2015).

worden. Es sei eine Illusion anzunehmen, Verbrechen in einer Gesellschaft gänzlich verhindern zu können. Am Bsp. des NSU-Prozesses[126] sei klar ersichtlich, dass Überwachung der Gesellschaft Verbrechen nicht verhindern könne. Die Wirkungslosigkeit der Überwachung im Kampf gegen Terrorismus habe Edward Snowden bestätigt.[127] Es sei daher zu unterstreichen, dass Überwachung nichts zur Verbrechensprävention beitrage.

Mod. RH: Aufruf der nächsten Frage.

Hörer_in: [an Vorredner_in] Der Vertrauenseinbruch gegenüber Geheimdiensten basiere auf einem sichtbaren Eigenleben der Geheimdienste, welches scheinbar keiner Instanz Rechenschaft schuldig sei. Bei verübten Verbrechen sei eine Unsicherheit darüber festzustellen, ob diese nicht vorsätzlich von Geheimdiensten initiiert worden seien, um sich selbst Daseinsberechtigungen zu verschaffen.[128] Daher müsse die Politik in die Pflicht genommen werden, Geheimdienste abzuschaffen. [Zuspruch aus der Hörer_innenschaft] In gleichem Maße müsse seitens der Politik die Schnüffelei der Privatwirtschaft unter Strafe gestellt werden.

Mod. RH: Aufruf der nächsten Frage.

Hörer_in: Klarstellung, das Anliegen des Ministeriums für Staatssicherheit sei es gewesen, einen gläsernen Menschen zu schaffen. Die Überwachungsmethoden hätten durchaus auch darauf abgezielt, das Leben der überwachten Personen bis in die kleinsten Bereiche hinein zu protokollieren, so bspw. auch Geruchsproben der Überwachten zu sichern.

Die aktuelle Datensammelwut finde auf zwei Ebenen statt. Die erste Ebene erfolge von staatlicher Seite, die zweite von Unternehmen. In der Überwachung durch private Unternehmen sei daher die neue Dimension der Überwachung zu sehen. Eine der spannendsten Voraussetzungen zur Aufarbeitung der Überwachungsaffäre bestehe darin zu beobachten, wie Nationalstaaten gegen die wirtschaftliche Überwachung durch Unternehmen vorgingen. Zumindest werde ein solches Vorgehen aktuell von Bürger_innen erwartet.

Mod. RH: Aufruf der letzten Frage.

Hörer_in: Die mutmaßlichen Haupttäter des Attentates in Paris vom 7. Jan. 2015 seien durch den Fund eines Personalausweises, den einer der Attentäter im Fluchtfahrzeug vergessen habe, ausfindig gemacht worden. Wäre es möglich gewesen, die Attentäter auch ohne diesen Zufallsfund zeitnah zu stellen?

Mod. RH: Eine letzte Frage aus der Moderation an NT, DrAK und DA für einen abschließenden Redebeitrag der Gastrednerinnen sei, welche Möglichkeiten Normalbürger_innen hätten, gegen Überwachung aktiv zu werden, berücksichtige man die zeitlichen Einschränkungen, die eine reguläre Arbeitswoche mit sich bringe, sodass für gesellschaftspolitisches Engagement kaum Zeit bleibe.

---

126 http://www.muenchen.de/aktuell/nsu-prozess.html (zuletzt aufgerufen: 17. Sep. 2015).

127 HOLLAND, M.: „Snowden: Massenhafte Datensammlung sinnlos gegen Terrror“, heise.de, 22. Jan. 2015, online abrufbar unter: http://www.heise.de/newsticker/meldung/Snowden-Massenhafte-Datensammlung-sinnlos-gegen-Terrror-2525837.html – Kurzlink: http://heise.de/-2525837 (zuletzt aufgerufen: 17. Sep. 2015).

128 Anm. d. Pr.: Vgl. bspw. zur Plutonium-Affäre / Operation Hades den Beschluss des Bundestages über die Einsetzung eines Untersuchungsausschusses vom 11. Mai 1995, online abrufbar unter: http://dipbt.bundestag.de/dip21/btd/13/013/1301323.pdf – Kurzlink: http://kurzlink.de/gLbBUOtxC (zuletzt aufgerufen: 17. Sep. 2015).

DA: Die Möglichkeiten zeigten sich an dieser Veranstaltung, in der unter der Überschrift „Vom Sinn der Überwachung“ eine Vielfalt an Fragen diskutiert worden sei, sodass zumindest für die Klärung der gesellschaftspolitischen Dimension der Überwachungsaffäre ein wenig Aufarbeitung habe stattfinden können. In diesem Zusammenhang sei es sehr wichtig, die Fragestellung des Digitalen Wandels an unsere Gesellschaft als eine sehr komplexe anzuerkennen. Diese habe sich in der Diskussion des heutigen Abends vorrangig auf die Innenpolitik konzentriert, könne aber bspw. bzgl. der Bildungspolitik ebenso umfangreich diskutiert werden. In keinem dieser Bereiche gäbe es Antworten, die das Problem der Überwachung einfach und schnell lösten, da Politik überaus kompliziert und extrem detailversessen sei. Dennoch könnten alle Bürger_innen zur Analyse des Problems beitragen. In der heutigen Veranstaltung habe diesbezüglich bereits eine Identifikation mehrerer Probleme der Überwachungsaffäre stattgefunden, die darüber hinaus in einigen Punkten dazu befähigt habe, individuelle Konsequenzen zu ziehen, sodass schließlich den diskutierten Missständen durch eine gestärkte digitale Mündigkeit der Bürger_innen begegnet werden könne. Der politische Prozess stehe im Rahmen des Digitalen Wandels erst am Anfang und werde beständig von einer sehr aktiven Netzgemeinde kritisiert und gefordert. Neben den Vorstellungen der Netzgemeinde müsse aber zugleich darauf geachtet werden, den weniger technikaffinen Teil der Bevölkerung im gesellschaftlichen Wandlungsprozess nicht zu verlieren. Für die Breite der Gesellschaft tragfähige Antworten seien entsprechend schwierig zu finden und umzusetzen. An der Entwicklung der Umweltbewegung sei aber zu erkennen, wie sich gesellschaftliches Umdenken langsam, aber stetig ausbreite. Der angesprochene Vergleich sei daher treffend gewesen, da auch Umweltaktivist_innen zunächst als paranoide Minderheit betrachtet worden seien. Deren Anliegen seien jedoch mittlerweile in der Breite der Gesellschaft angekommen und hätten zu umfangreichen politischen Kursänderungen geführt. Über das Anfangsstadium netzpolitischer Forderungen sei man jedoch bereits hinaus, da durch die Enthüllungen von Edward Snowden das Anliegen einer kleinen Minderheit von Informatiker_innen einen bedeutenden Aufschwung erhalten habe. Die Herausforderung bestehe nun darin, die gewonnene netzpolitische Aufmerksamkeit einzusetzen, um Reformprozesse einzuleiten, die eine gesamtgesellschaftliche Hebelwirkung hätten.

Zu den einzelnen Fragestellungen meinte DA erstens, sie sei eine Verfechterin einer umfangreichen Bildungsinitiative, um den Herausforderungen des Digitalen Wandels zu begegnen. Sie befürworte einen reformierten Informatikunterricht und erweiterte berufliche Bildung, die dazu diene, erworbene Qualifikationen im Zuge technischen Fortschritts zu erhalten. Dieser Herausforderung begegne DA bspw. in Zusammenarbeit mit Saskia Esken in einer Arbeitsgruppe zum Thema „Digitale Bildung“.[129]

Zweitens müsse zur Rolle der Geheimdienste die Frage nach der Kontrolle von Geheimdiensten gestellt werden. Geheimdienste hätten ihre aktuellen Strukturen in der Zeit des Kalten Krieges erhalten, die entsprechend überdacht werden müssten. Die Forderung, Geheimdienste schlicht abzuschaffen, sei zu einfach gedacht. Zwar hätte sich bisher niemand getraut, die etablierten Geheimdienststrukturen zu

129 https://netzpolitik.bayernspd.de/ (zuletzt aufgerufen: 18. Sep. 2015).

verändern, der NSA-Untersuchungsausschuss habe jedoch das Potential, Geheimdienstreformen anzustoßen, sofern dies mutig erfolge.

Drittens erwarte DA von der Politik, das Problem der Überwachungsaffäre zu verstehen. Der dazu notwendige Überzeugungsvorgang müsse von allen Bürger_innen in ihrer jeweiligen gesellschaftlichen Interaktion immer wieder angestoßen werden.

Viertes müsse die Hilfe zur Selbsthilfe innerhalb des Digitalen Wandels die zentrale Forderung an die Politik sein. Diese könne über eine entsprechende Bildungspolitik erfolgen, wofür jedoch die Förderung von sicheren Kryptographiealgorithmen nötig sei, die sowohl dem Schutz der Bevölkerung als auch der Industrie dienlich seien.

DrAK: Die Überwachungsaffäre müsse als Gesprächsthema in den Räumen zwischenmenschlicher Gemeinschaft aktuell gehalten werden, um Aufklärungsarbeit voranzutreiben. Der Öffentlichkeit müsse das Thema bewusst bleiben, damit Überwachung als Störung der Gesellschaft insgesamt empfunden werde.

Die ausbleibenden Erfolge von Überwachung zur Verbrechensbekämpfung sei allem Anschein nach auf die seltsame Verwertung der Überwachungsdaten zurückzuführen. Eine intelligente Auswertung zur Verbrechensbekämpfung scheine nicht stattzufinden, wohl aber die Verwertung der Daten zugunsten des Erhalts einer sich abzeichnenden Willkürherrschaft. Diese setze Kriterien, nach denen Menschen klassifiziert und als verdächtig eingestuft würden. Die aktuelle Lage zwinge förmlich zum Bild einer Gesellschaft unter Generalverdacht, in der jedes Individuum dem Vorwurf unterliege, etwas zu verbergen zu haben, da anders der status quo einer anlasslosen Massenüberwachung nicht zu erklären sei.

[Zuspruch aus der Hörer_innenschaft]

Hörer_in: Grundsätzlich stünden zwei Personengruppen in der Pflicht. Zum einen sei die Politik in der Pflicht, gegen staatliche Überwachung aufzuklären und gegen diese gesetzlich zu schützen. Für das Problem der privatwirtschaftlichen Überwachung trage zwar ebenfalls die Politik eine Verantwortung, es obliege jedoch vor allem den Bürger_innen die Entscheidung, sich aktiv, bspw. in der Art und Weise des Umgangs mit dem Smartphone, privatwirtschaftlicher Überwachung zu entziehen. Auch hier sei eine Bildungspolitik der Schlüssel zur Erziehung mündiger Bürger_innen.

Mod. RH: Überleitung zum Abschluss der Veranstaltungsabends. Danksagung an die Gastrednerinnen unter Applaus der Hörer_innenschaft. Einladung zur letzten Praxisveranstaltung zum „Datenschutz und Datenhoheit ohne Verschlüsselungstechniken“. Einladung, die unter einer freien Nutzungslizenz erstellten Dokumente der Initiative für eigene Weiterbildungsprojekte zu nutzen. Bitte um Kritik und Fotografien des Abends per E-Mail (Folie 16).

Abschluss

Zum Abschluss der Veranstaltung solle mit dem bekanntesten Mitgründer des Unternehmens Apple ein „IT-Prophet“ aus den achtziger Jahren zu Wort kommen. Dieser habe im Jahr 1983 das Unternehmen IBM herausfordern wollen, als die noch junge Firma Apple ihren neuen Computer „Macintosh“ vorstellte.

Während dieser Produktvorstellung habe sich Steve Jobs im damals präsentierten Werbefilm für Anspielungen auf die Konkurrenz aus dem Roman „1984“ von George Orwell bedient (Folie 17).[130] Nachfolgend findet sich die Transkription des in der Veranstaltung eingespielten Videos (Folie 18):

Exkurs: „1984“ in der Rezeption von Apple Inc.

Zeitindex	Englisch	Deutsch
00:03:20	It is now 1984. It appears IBM wants it all.	Wir haben nun das Jahr 1984. IBM will scheinbar alles haben.
00:03:30	Apple is perceived to be the only hope to offer IBM a run for its money.	Apple wird als einziger Kandidat gesehen, der in der Lage ist, IBM einen Wettkampf zu bieten.
00:03:36	Dealers, initially welcoming IBM with open arms, now fear an IBM-dominated and controlled future.	Händler haben IBM zunächst mit offenen Armen empfangen. Jetzt fürchten sie sich vor einer Zukunft, die von IBM beherrscht und gesteuert wird.
00:03:44	They are increasingly and desperately turning back to Apple as the only force that can ensure their future freedom. [applause]	Sie wenden sich zunehmend, und mit immer größerer Verzweiflung, an Apple zurück. Apple betrachten sie als die einzige Macht, die ihre künftige Freiheit sichern kann. [Applaus]
00:04:00	IBM wants it all, and is aiming its guns on its last obstacle to industry control: Apple.	IBM will alles haben, und zielt mit ihrem Gewehr auf das letzte Hindernis für ihre Herrschaft der Branche: Apple.
00:04:09	Will “Big Blue” dominate the entire computer industry [audience member: No!], the entire information age [audience: No]?	Wird „Big Blue“ die ganze Computerbranche dominieren [Zuschauer: „Nein!“], das ganze Informationszeitalter dominieren [Publikum: „Nein“]?
00:04:18	Was George Orwell right about 1984? [applause]	Hatte George Orwell Recht bezüglich 1984? [Applaus]
00:04:25	[Begin of “1984” advertisement] For today, we celebrate the first glorious anniversary of the Information Purification Directives.	[Beginn „1984“ Werbefilm] Heute feiern wir das erste Jubiläum der „Information Purification Directives“ [Anordnungen zur Informationsreinigung].
00:04:32	We have created – for the first time in all history – a garden of pure ideology, where each worker may bloom, secure from the pests purveying contradictory thoughts.	Zum ersten Mal in der Geschichte haben wir einen Garten der reinen Ideologie erschaffen, in dem jeder Arbeiter erblühen kann, geschützt von den Schädlingen, die widersprechende Gedanken verbreiten.
00:04:46	Our unification of thoughts is more powerful a weapon than any fleet or army on Earth.	Als Waffe ist die Vereinigung unserer Gedanken mächtiger als alle Flotten und Armeen dieser Erde.
00:04:53	We are one people, with one will, one resolve, one cause.	Wir sind ein Volk mit einem Wille, einer Entschlossenheit, einem Beweggrund.
00:05:00	Our enemies shall talk themselves to death, and we will bury them with their own confusion. We shall prevail.	Unsere Feinde werden sich mit Gerede zum Tode führen und wir werden sie mit ihrer eigenen Verwirrung beerdigen. Wir werden siegen.
00:05:14	On January 24th, Apple Computer will	Am 24. Januar wird Apple Computer den Macintosh

130 Der in der Veranstaltung eingespielte Ausschnitt bezieht sich auf den Zeitindex 00:03:20-00:05:29 des Beitrages „1983 Apple Keynote-The "1984" Ad Introduction“, online abrufbar über The Apple History Channel unter: https://youtu.be/ISiQA6KKyJo?t=3m20s (zuletzt aufgerufen: 18. Sep. 2015).

	introduce Macintosh. And you'll see why 1984 won't be like *1984*.	vorstellen. Und sie werden sehen, wieso 1984 anders sein wird als „1984“.
00:05:17- 00:05:29	[Applause]	[Applaus]

Exkurs: „1984“ in der Rezeption der NSA

Steve Jobs habe sich 1983 mit Idealismus aus den Inhalten von „1984“ bedient, um provokativ den eigenen Anspruch zu verdeutlichen, Verfechter einer freien Welt zu sein. Durch die Snowden-Enthüllungen sei bekannt, dass auch die NSA sich des Stoffes von „1984“ bediente, jedoch in einer befremdlich anderen Weise (Folien 19-21).[131]

So stelle die NSA auf einer ursprünglich geheimen Präsentation, die auf den eben gezeigten 1983er Werbefilm von Apple anspiele, die Frage, wer es im Jahr 1984 für möglich gehalten habe (Abb. 1), dass dies, gemeint ist das iPhone, einmal der „große Bruder“ (Abb. 2) und die „Zombies“, also die im Werbefilm gezeigten willenlosen Menschengestalten, eine zahlende Kundschaft sei (Abb. 3). Dabei stehe Apple nur exemplarisch für einen Informationsgiganten neben Amazon, eBay, Facebook, Google, Microsoft oder Yahoo. Es solle

Abb. 1: Photo Gallery: Spying on Smartphones 1/5, spiegel.de, online abrufbar unter: http://www.spiegel.de/fotostrecke/photo-gallery-spying-on-smartphones-fotostrecke-101201.html (zuletzt aufgerufen: 18. Sep. 2015).

Abb. 2: Photo Gallery: Spying on Smartphones 2/5, spiegel.de, online abrufbar unter: http://www.spiegel.de/fotostrecke/photo-gallery-spying-on-smartphones-fotostrecke-101201-2.html (zuletzt aufgerufen: 18. Sep. 2015).

Abb. 3: Photo Gallery: Spying on Smartphones 3/5, spiegel.de, online abrufbar unter: http://www.spiegel.de/fotostrecke/photo-gallery-spying-on-smartphones-fotostrecke-101201-3.html (zuletzt aufgerufen: 18. Sep. 2015).

nicht ausgeschlossen werden, dass diese Unternehmen einmal tugendhafte Absichten hatten, sie jedoch schließlich Hand in Hand mit den Geheimdiensten arbeiteten[132] und demnach höchstens Empörung vorspielten, seit ihre geheimdienstlichen Verstrickungen durch Snowden bekannt geworden

131 Angaben der Folien dieses Abschnitts s. Anhang 5 »„Vom Sinn der Überwachung“ – Präsentationsfolien der Veranstaltung«.

seien. RH bedanke sich bei der Hörer_innenschaft für die rege Teilnahme und hoffe, die Initiative habe inspirieren können, das Unrecht der globalen Überwachungsaffäre weiter zu reflektieren, um Konsequenzen in privater, öffentlicher und politischer Hinsicht zu ziehen.

[Applaus der Hörer_innenschaft]

132 MacAskill, E.: „NSA paid millions to cover Prism compliance costs for tech companies“, theguardian.com, 23. Aug. 2013, online abrufbar unter: http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid – Kurzllink: http://kurzlink.de/Gr2QoKfTh (zuletzt aufgerufen: 18. Sep. 2015).

Humboldt-Universität zu Berlin
Jacob-und-Wilhelm-Grimm-Zentrum
Studentische Initiative „Jahr 1 nach Snowden“
Praxisveranstaltung I – „Rollentausch: (sich) selbst überwachen!“ (17. Nov 2014 – WiSe 2014/15)

Entwurf zur Praxisveranstaltung I – „Rollentausch: (sich) selbst überwachen!“

Tutoren: Amon Kaufmann (kaufmann@physik.hu-berlin.de)
Roland Hummel (roland.hummel@theologie.hu-berlin.de)
Autor: Roland Hummel

Zeitfenster	Inhalt	Unterrichts-form	Regieanweisungen und Notizen
17:00-19:00 (120min)	1. Zeitplan an die Tafel 2. Computer checken 3. Software ggf. nachinstallieren 4. Präsentation starten mit Hinweis „Computer nicht ummelden“	**Vorbereitung**	
19:15-19:30 (15min) **Einstieg**	1. Gang zum Schulungsraum 2. Kurzvorstellung Initiative 3. Wer wir sind (keine Informatiker) 4. Was wir heute machen („prism yourself“ für Einsteiger) und was wir nicht machen (Unterschied Hacker/Cracker) 5. Zeitplan erklären (Pausenhinweis) 6. Ausgang und Toiletten 7. Fragen?	Lehrervortrag	- Stichworte an Tafel schreiben
19:30-20:10 (40min) **Theorie**	1. Soziales Netzwerk analysieren mit **Facebook** und **NameGenWeb** Bsp.: Amons Account bis **19:40** (10min)	Lehrervortrag	- Namen und Links zweiter Beamer Facebook: https://www.facebook.com/ NameGenWeb: https://apps.facebook.com/namegenweb/
	2. E-Mail-Metadaten analysieren mit **GMail** und **Immersion** (MIT) sowie **MUSE** (Stanford) Bsp.: Demo (Immersion) oder Rolands Account (Stanford) bis **19:50** (10min)	Lehrervortrag	- Namen und Links zweiter Beamer Immersion: https://immersion.media.mit.edu/ MUSE: http://mobisocial.stanford.edu/muse/
	3. Webseitenstruktur „**crawlen**“ mit Crawler von **webmasterworld.com** Bsp.: jahr1nachsnowden.de bis **20:00** (10min)	Lehrervortrag	- Name und Kurzlink zweiter Beamer webmasterworld.com: http://kurzlink.de/MdMY2TipL jahr1nachsnowden.de http://www.jahr1nachsnowden.de
	4. **Profilanalyse** mit **Google-Standardsuche** Bsp.: Freiwilliger und/oder Roland Hinweis: Google-Operatoren nutzen bis **20:10** (10min)	Lehrervortrag	- Namen und Links zweiter Beamer Google: https://www.google.de/ Google-Operatoren: http://kurzlink.de/Es3vEs8O5 - Amons Profil aufheben für Praxis-Teil

	Puffer 1: Falls Freiwilliger: Aufenthaltsort von Twitter-Nutzern herausfinden mit **pleaserobme.com** bis **max. 20:10**	Lehrervortrag	- Name und Link zweiter Beamer pleaserobme.com: http://pleaserobme.com/
	Puffer 2: Lokation der eigenen Position je nach Verbindung mit **sempervideo.de/geo** Hinweis: Unterschied LAN/WLAN/VPN bis **max. 20:10**	Lehrervortrag	- Namen und (Kurz-)Links zweiter Beamer sempervideo.de/geo: http://www.sempervideo.de/geo/ Youtube-Video: http://kurzlink.de/e0ZfzAVQa
	Puffer 3: Unverschlüsselten Datenstrom auslesen mit **Wireshark** Bsp.: test.moodle2.de bis **max. 20:10**	Lehrervortrag	- Namen und Links zweiter Beamer Wireshark: https://www.wireshark.org/ Testseite Theorie: http://test.moodle2.de/ Testseite Praxis: http://demo.moodle.net/login/index.php
20:10-20:20 (10min)	Hinweis für Getränkeautomat und Toiletten	**Pause**	
20:20-20:50 (30min) **Praxis1**	- Hinweis: Praxis-Teil einzeln oder in Gruppenarbeit - Hinweis: bei Fragen immer fragen **Möglichkeit 1**: keine Aufgaben, genannte Möglichkeiten selbst ausprobieren **Möglichkeit 2**: Aufgaben: 1. (falls vorhanden:) Analysiere die sozialen Verbindungen deines **Facebook**-Profils 2. Analysiere die Korrespondenz deines **GMail**-Accounts mit **Immersion** oder **MUSE** 3. **„Crawle“**, womit sich z. B. folgende Seiten auseinandersetzten, ohne sie direkt zu besuchen: - roland-schmidt.com - heldenwelt.de 4. Schätze die Gefahr von getwitterten Aufenthaltsorten mittels **pleaserobme.com** ein 5. Google, was **Amon** neben dem Physikstudium eventuell noch macht oder gemacht hat	Einzel- oder Gruppenarbeit	- präsent sein - Einzelfragen für Reflexionsteil sammeln Links für Aufgaben nach Reihenfolge: 1. NameGenWeb: https://apps.facebook.com/namegenweb/ 2. Immersion: https://immersion.media.mit.edu/ + MUSE: http://mobisocial.stanford.edu/muse/ 3. Crawlen: http://kurzlink.de/MdMY2TipL 4. PleaseRobMe.com: http://pleaserobme.com/ 5. Google-Operatoren: http://kurzlink.de/Es3vEs8O5 6. Wireshark: https://www.wireshark.org/

	6. Alles langweilig? Frage nach einem Auftrag für **Wireshark**.		+ Testseite Praxis: http://demo.moodle.net/login/index.php
20:50-21:00 (10min) **Reflexion**	1. Beobachtete Probleme und Fragen klären 2. Ersteindruck in Bezug auf die demonstrierten Möglichkeiten erfragen 3. Hinweis auf Dimension von PRISM&Co	Lehrer-Schüler-Gespräch	- einer moderiert, der andere schreibt Stichworte an die Tafel -Hinweis Snowden-Akten auf Spiegel.de: http://kurzlink.de/K7XguXEcn
21:00-21:20 (20min) **Praxis2**	Zeit, um weiteres Projekt auszuprobieren, Empfehlung: 1. **heise.de/netwars** 2. **thenetworkiswatching.com** 3. **panopticlick.eff.org**	Einzel- oder Gruppenarbeit	1. http://www.heise.de/extras/netwars/ 2. http://www.thenetworkiswatching.com/ (1. und 2. besser mit Kopfhörern) 3. https://panopticlick.eff.org
21:20-21:30 (10min) **Abschluss**	Gedanken zum „Rollentausch“: 1. nicht zum Angriff, sondern zur **Verteidigung** 2. **Trilemma** beachten: • komfortabel • kostenlos • datenschonend -> zwei bekommt man, eines i. d. R. nicht! 3. weiter **informieren** (ab und zu z. B. **sempervideo.de** statt Tagesschau/Serie) 4. gesellsch. **Situation** relativieren: *„Hope the best, expect the worst!“* 5. Ausblick: **Komfortzone** verlassen, digitale **Zivilcourage** (sein eigenes „digitales Ich“ schützen und das der Anderen)	Lehrervortrag	- ev. Flyer und Infomaterial austeilen

1 ## Linkverzeichnis

URL (alphabetisch n. Anfangsbuchstaben der Domainnamen, z. B. https://www.facebook.com/])	Kurz-Link
https://panopticlick.eff.org	
https://www.facebook.com/	
https://apps.facebook.com/namegenweb/	
https://www.google.de/	
https://immersion.media.mit.edu/	
http://www.onlinemarketing-praxis.de/uploads/pdf/suchparameter-google-uebersicht.pdf	http://kurzlink.de/Es3vEs8O5
http://pleaserobme.com/	
http://www.sempervideo.de/geo/ \-> Erklärung unter: https://www.youtube.com/watch?v=hEvFQRNzwAM	http://kurzlink.de/e0ZfzAVQa
http://www.spiegel.de/netzwelt/web/snowdens-deutschland-	http://kurzlink.de/K7XguXEcn

akte-alle-dokumente-als-pdf-a-975885.html	
http://mobisocial.stanford.edu/muse/	
http://www.thenetworkiswatching.com/	
http://freetools.webmasterworld.com/tools/crawler-google-sitemap-generator/	http://kurzlink.de/MdMY2TipL
https://www.wireshark.org/ \-> am Bsp.: http://test.moodle2.de/	

Humboldt-Universität zu Berlin
DJV Berlin e.V. - Landesverband des Deutschen Journalisten-Verbandes
Studentische Initiative „Jahr 1 nach Snowden“
Praxisveranstaltung II – „Einführung in verschlüsselte Kommunikation“ (15. Dez 2015 – WiSe 2014/15)

Entwurf zur Praxisveranstaltung II – „Einführung in verschlüsselte Kommunikation“

Initiatoren: Amon Kaufmann (kaufmann@physik.hu-berlin.de)
Roland Hummel (roland.hummel@theologie.hu-berlin.de)
Tutor und Autor: Roland Hummel

Zeitfenster	Inhalt	Unterrichts-form	Regieanweisungen und Notizen
17:30-19:00 (90min) **Vorbereit.**	1. RollUp aufstellen 2. Zeitplan + WLAN an die Tafel 3. Eigene Technik und Beamer testen 4. Pro Person 2 Zettel vorbereiten u. verteilen 5. Präsentation starten mit Hinweis 1. WLAN-Zugang, 2. GnuPG-Installation, 3. E-Mail-Zettel bis 19:00 (90min)	Vorbereitung	Zu 5.) GnuPG: https://www.gnupg.org/download/index.html
19:15-19:30 (15min) **Einstieg**	1. Kurzvorstellung **Initiative** und **Tutor** 2. **Was** wir heute machen (Thunderbird/Enigmail für Einsteiger) und was wir **nicht** machen (Outlook/AppleMail/Android/„Mathematik“) 3. **Zeitplan** erklären (Pausenhinweis), Ausgang und Toiletten 4. 1. **Zettel** Name und E-Mailadresse (**öffentlich**) – 2. Zettel PGP-Daten (**privat**) 5. **Motivation** VS Komplexität: OpenPGP für selbstbestimmte, dezentrale, transparente Verschlüsselung VS zentralisierte Systeme außerhalb der Nutzerkontrolle bis 19:30 (15min)	Lehrervortrag	
19:30-20:10 (40min) **Theorie**	1. Unterschied **symmetrischer und asymmetrischer** Verschlüsselung bis 19:35 (5min)	Lehrervortrag	- Hinweis: **„Bitte ersteinmal nur zuschauen!“** - ev. Demo mit CrypTool2
	2. Unterschied **Verschlüsseln** und **Signieren** bis 19:40 (5min)	Lehrervortrag	
	3. **Zentrales** und **dezentrales** Signieren bis 19:45 (5min)	Lehrervortrag	
	4. Dezentral: „Web of Trust“ (**WoT**) bis 19:50 (5min)	Lehrervortrag	
	5. Bsp mit **Thunderbird** und **Enigmail** - Wizard folgen: 5.1 „für alle Identitäten?“ - ja 5.2 „immer verschlüsseln?“ - sofern Key schon vorhanden, ja (1. Option)	Lehrervortrag	

	5.3 „immer signieren?“ - nein (erstmal nicht) 5.4 „Einstellungen angleichen“? - ja 5.5 „Neues Schlüsselpaar erstellen?“ - ja 5.6 Account/ID auswählen – Passwort wählen 5.7 Zusammenfassung bestätigen 5.8 Schlüsselerzeugung abwarten 5.9 „Widerrufszertifikat erstellen?“ - ja (Passwort bei Abfrage *nie* speichern, Warnung bestätigen, fertig) 5.10 öffentlichen Schlüssel veröffentlichen 5.11 Schlüsselpaar sichern / drucken 5.12 Widerrufsfunktion zeigen bis 20:00(10min)		Zu 5.6) Passwortcheck mit: http://www.cryptool-online.org/index.php?option=com_cto&view=tool&Itemid=159&lang=de Kurzlink: http://kurzlink.de/vuaf2BL6M (PW kann nachträglich geändert werden) Zu 5.10) klassisch **per E-Mail** verschicken oder auf **Keyserver** hochladen (ist dort aber mitunter nicht sofort öffentlich abrufbar)
20:00-20:10 (10min) Pause	Hinweis für Getränke und Toiletten bis 20:10 (10min)	Pause	
20:10-20:55 (45min) **Praxis1**	1. **GnuPG** und **Enigmail** installieren - Neustart Thunderbird - Wizard folgen: 1.1 „für alle Identitäten?“ - ja 1.2 „immer verschlüsseln?“ - sofern Key schon vorhanden, ja (1. Option) 1.3 „immer signieren?“ - nein (erstmal nicht) 1.4 „Einstellungen angleichen“? - ja 1.5 „Neues Schlüsselpaar erstellen?“ - ja 1.6 Account/ID auswählen – Passwort wählen 1.7 Zusammenfassung bestätigen 1.8 Schlüsselerzeugung abwarten 1.9 „Widerrufszertifikat erstellen?“ - ja (Passwort bei Abfrage *nie* speichern, Warnung bestätigen, fertig) 1.10 öffentlichen Schlüssel veröffentlichen 1.11 Schlüsselpaar sichern / drucken 1.12 Widerrufsfunktion zeigen bis 20:30 (20min)	Schülerarbeit	GnuPG: https://www.gnupg.org/download/index.html Zu 1.6) sichere(re)s Passwort mit: http://www.cryptool-online.org/index.php?option=com_cto&view=tool&Itemid=159&lang=de Kurzlink: http://kurzlink.de/vuaf2BL6M (PW kann nachträglich geändert werden) Zu 1.10) klassisch **per E-Mail** verschicken oder auf **Keyserver** hochladen (ist dort aber mitunter nicht sofort öffentlich abrufbar)
	2. E-Mail an **Sitznachbar** (Uhrzeigersinn) 2.1.1 entweder sofort verschlüsselt mit Keyserver-Suche (falls schon zu finden) 2.1.2 ggf. unverschlüsselte, aber schon signierte E-Mail mit Zusendung des öffentlichen Schlüssels	Schülerarbeit	Zu 2.) **öffentlichen** Zettel *im* Uhrzeigersinn rotieren lassen (jeder hat Name und E-Mail seines Nachbarn) Zu 2.2.1) SKS-Keyserver-Interaktion: https://sks-keyservers.net/i/ (ev. Signatur-Warnung, kann auf *dieser* Seite ignoriert

	2.2 Schlüssel importieren 2.3 E-Mail verschlüsselt und signiert beantworten bis 20:40 (10min)		werden)
	3. **Signatur-Warnung** beachten und entsprechend Zertifizierung mit Sitznachbar mittels **Fingerprint** auf öffentlichem **Zettel** 3.1 Zettel mit Fingerprints vergleichen Schlüsselverwaltung+öffentlicher Zettel oder Schlüsselverwaltung+Schlüsselserver 3.2 digital unterschreiben/signieren 3.3 **Owner Trust**/Besitzer-Vertrauen festlegen Wichtige Hinweise dazu: 1. **Korrekte Signierung** ist durchaus komplizierter Teil: Verständnis nötig für Optionen in Bezug auf „**Sign Key**“/“Schlüssel unterschreiben“ und „Set **Owner Trust**“/“Besitzer-Vertrauen festlegen“, beide Angaben fließen in die (immer individuelle) Berechnung der „**Key validity**“/ „Schlüsselgültigkeit“ (siehe Eigenschaften eines Schlüssels in Schlüsselverwaltung) ein für das immer eigene, daher *immer individuelle* WoT 2. **Optionen** nicht unbedingt selbsterklärend, Online-Erklärungen wie z. B. https://de.wikipedia.org/wiki/Web_of_Trust#Owner_Trust recht kompliziert, auch diese hier dient nur der ersten Orientierung und erhebt *keinen* Anspruch auf Richtigkeit → unbedingt selbst alle paar Wochen damit beschäftigen, damit sich das Verständnis verdichtet bis 20:50 (10min)	Schülerarbeit	**Zu 3.1) Fingerprint** abgleichen: 1. *öffentlichen* Zettel *gegen* Uhrzeigersinn an Besitzer zurück 2. Zettelbesitzer schreibt Fingerprint *seines* öffentlichen Schlüssels auf den Zettel 3. *öffentlichen* Zettel nochmals *gegen* Uhrzeigersinn an Sitznachbar geben (Empfänger meiner Nachricht hat jetzt meinen Fingerprint auf meinem Zettel) 4. Sitznachbar gleicht Fingerprint von meinem Zettel mit Fingerprint in Schlüsselverwaltung/Schlüsselserver ab → sollte übereinstimmen, sofern keine Schreibfehler, sodass Überprüfung erfolgreich (Schlüssel gehört sicher demjenigen, der vorgibt, ihn erstellt zu haben – es spricht nichts dagegen bei persönlichen Treffen zur Prüfung des Schlüssels auch noch einen Ausweis hinzuzuziehen) **Zu 3.2)** Optionen „**Sign Key**“/“Schlüssel unterschreiben“: 1. „I will not answer“/„Keine Antwort“ (=**sig0**) 2. „I have not checked at all“/„Ich habe es nicht überprüft“ (=**sig1**) 3. „I have done casual checking“/„Ich habe es nur einfach überprüft“ (=**sig2**) 4. „I have done very careful checking“/ „Ich habe es sehr genau überprüft“ (=**sig3**) **-› öffentliche Info** für Schlüsselserver! [5. Option „Local signature (cannot be exported)“/“Lokal unterschreiben (nicht exportierbar) → Unterschrift bleibt lokal] **Zu 3.3)** Optionen „Set **Owner Trust**“/“Besitzer-Vertrauen festlegen“ 1. „I don't know“/„unbekannt“ (Standard) 2. „I do NOT trust“/„kein Vertrauen“ 3. „I trust marginally“/„geringes Vertauen“ 4. „I trust fully“/„volles Vertrauen“ 5. „I trust ultimately“/„absolutes Vertrauen“ → diese Vertrauenskategorie bezieht sich auf Schlüssel**ersteller** und wird **nie veröffentlicht** (ist auch nicht nötig)!
	4. E-Mail beantworten und **positive Signatur-Meldung** beachten bis 20:55 (5min)	Schülerarbeit	
20:55-20:05 (10min) **Reflexion**	1. Wichtige **Fragen** klären 2. Komplexität reflektieren: drei wichtige Aspekte für erfolgreiche Verschlüsselung: I – sichere **Technik**	Lehrer-Schüler-Gespräch	

	II – sicherer **Umgang** III – **Konsequenz** in der Anwendung 3. Belohnung: **Unabhängiges, selbstverwaltetes Verfahren** und **„Sand im Getriebe“** der Massenüberwachung 4. Verschlüsselter E-Mail**versand** für Leute, die kein PGP nutzen: encrypt.to bis 21:05 (10min)		Zu 4.) encrypt.to: https://encrypt.to/
21:05-21:20 (15min) **Praxis2**	2 Möglichkeiten: 1. *Öffentlichen* Zettel nochmals mit anderem Partner tauschen und Schritte wiederholen 2. Verständnistest ablegen: openpgp-schulungen.de/verstaendnistest bis 21:20 (15min)	Einzel- oder Gruppenarbeit	Zu 2.) openpgp-schulungen.de: http://openpgp-schulungen.de/verstaendnistest/
21:20-21:30 (10min) **Abschluss**	**Abschlussgedanken** zur Kryptographie: 1. Nur **eine Möglichkeit unter vielen**, aber eine sehr sichere, eigenverantwortliche 2. **Trilemma** gilt auch bei Verschlüsselungsprogrammen: • komfortabel • kostenlos • sicher -> max. zwei bekommt man! 3. Drei wichtige Aspekte für Verschlüsselung: I – sichere **Technik** II – sicherer **Umgang** III – **Konsequenz** in der Anwendung 4. **Absicherung** der Rechner (PGP schützt nicht vor Spionage auf Sende- und Empfangseinheiten, wenn die E-Mails geschrieben/entschlüsselt werden) 5. **Komfortzone** verlassen, digitale **Zivilcourage:** Sein eigenes „digitales Ich“ schützen und das der Anderen (auch fernab von Verschlüsselung in Praxisveranstaltung3) 7. Hinweis Hilfe auf amor.cms.hu-berlin.de/~paetzela und german-privacy-fund.de/e-mails-verschlusseln-leicht-gemacht 8. **Spendenaufruf** und **Bitte um Werbung**	Lehrervortrag	Zu 7.) HU-Seite: http://amor.cms.hu-berlin.de/~paetzela/ PGP in 30min:

	bis 21:30 (10min)		http://kurzlink.de/1oSwce2vd Zu 8.) ev. Flyer und Infomaterial austeilen

Linkverzeichnis

URL (alphabetisch n. Anfangsbuchstaben der Domainnamen, z. B. https://www.gnupg.com/])	Kurz-Link
https://www.cryptool.org/de/ (CrypTool2)	
https://encrypt.to/	
http://www.cryptool-online.org/index.php?option=com_cto&view=tool&Itemid=159&lang=de	http://kurzlink.de/vuaf2BL6M
http://www.german-privacy-fund.de/e-mails-verschlusseln-leicht-gemacht/	http://kurzlink.de/1oSwce2vd
https://www.gnupg.org/download/index.html	
http://amor.cms.hu-berlin.de/~paetzela/	
http://www.openpgp-schulungen.de/verstaendnistest/	
https://sks-keyservers.net/i/	
https://de.wikipedia.org/wiki/Web_of_Trust#Owner_Trust	

Humboldt-Universität zu Berlin
Jacob-und-Wilhelm-Grimm-Zentrum
Studentische Initiative „Jahr 1 nach Snowden“
Praxisveranstaltung III – „Datenhoheit und Datenkontrolle“ (19. Jan. 2015 – WiSe 2014/15)

Entwurf zur Praxisveranstaltung III – „Datenhoheit und Datenkontrolle“

Tutoren: Amon Kaufmann (kaufmann@physik.hu-berlin.de)
Roland Hummel (roland.hummel@theologie.hu-berlin.de)
Autor: Roland Hummel

Zeitfenster	Inhalt	Unterrichts-form	Regieanweisungen und Notizen
17:00-19:00 (120min) **Vorbereit.**	1. RollUp aufstellen 2. Zeitplan an die Tafel + Türproblem 3. Eigene Technik und Beamer testen **4. Programme testen (Tor und YaCy)** 5. Präsentation starten + Hinweis „Bitte noch nicht anmelden!“ 6. Rechner checken bis 19:00 (120min)	Vorbereitung	
19:15-19:30 (15min) **Einstieg**	1. **Begrüßung** mit Kurzvorstellung **Initiative** und **Tutor** 2. **Türproblematik** erklären 3. **Zeitplan** erklären (Pausenhinweis), Ausgang und Toiletten 4. **Was** wir heute machen (Möglichkeiten Datenschutz fernab von Verschlüsselung) 5. **Erst Theorie**-, dann Praxisteil (→ erstmal nur zuhören) 6. Hinweis: „Einführung in Linux“ quasi inklusive, da **Arbeitsrechner unter Linux** 7. **Theorieteil** vorstellen und nach **Fokus** fragen, da Zahl an **Maßnahmen immens** bis 19:30 (15min)	Lehrervortrag	- Namen und Links zweiter Beamer:: zu 6.) http://www.linuxmint.com/ http://distrowatch.com/
19:30-20:10 (40min) **Theorie**	1. Sichere(re) **Passwörter** → Problem: Verwendung von Geheimnissen zur Authentifizierung eigentlich absurd, aber finanziell attraktiv **2. 3 Konzepte** 2.1 **starkes** PW am Bsp. **passwordmeter.com**: PRO → punktuell sicher CON → langfristig unsicher sobald ein Dienst kompromittiert wurde 2.2 **Master-Passwort** oder „viele PW durch ein PW“ am Bsp. **masterpasswortapp.com**: PRO → sehr sichere PW → open source CON	Lehrervortrag	- Namen und Links zweiter Beamer:: zu 2.1) http://www.passwordmeter.com/ zu 2.2) http://masterpasswordapp.com/

	→ „alle Eier in einem Korb“-Problem maxim. → „Namensproblematik“ der Einträge 2.3 **Passwortcontainer** am Bsp. **KeePass Password Safe** 2.4 Hinweis auf **weiterführende Artikel** bis **19:40** (10min)		zu 2.3) http://www.keepass.info/
	1. Sichere(re)s **Surfen** mit erweitertem **Firefox** 2. Auswahl aus den Add-ons des Tutors: 2.1 Adblock Edge 2.2 anonymoX 2.3 CanvasBlocker 2.4 Flagfox 2.5 HTTPS-Everywhere 2.6 **NoScript** (VS Ghostery) am Bsp. **wikipedia.de** und der „Bäckereikarte“ von **zeit.de** → **zeit.de** → yieldlab.net → brightcove.com → t4ft.de → googletagmanager.com → **mapbox.com** → **jquery.com** → ioam.de Nack Freigabe von zeit.de zusätzlich: → krxd.net → nuggad.net → research.de.com 2.7 Self-Destructing Cookies 2.8 **mywot.com** bis **19:50** (10min)	Lehrervortrag	- Namen und Links zweiter Beamer: zu 2.1) http://kurzlink.de/KZPGXT4kI zu 2.2) http://kurzlink.de/OgDMc1Csa zu 2.3) http://kurzlink.de/LhRbpqP41 zu 2.4) http://kurzlink.de/hKcboB2fh zu 2.5) https://www.eff.org/https-everywhere zu 2.6) NoScript: http://kurzlink.de/BzUyxE2U2 zeit.de: http://kurzlink.de/3NLnhu1Mx (→ zeit.de) → http://www.yieldlab.de/ → https://www.brightcove.com/ → http://www.t4ft.de/ → googletagmanager.com → https://www.google.com/tagmanager/ → https://www.mapbox.com/ → https://jquery.com → ioam.de → https://www.infonline.de/ Nach Freigabe von zeit.de → krxd.net → http://cookiepedia.co.uk/host/krxd.net → http://www.nuggad.net/ → research.de.com → http://www.meetrics.com/ zu 2.7) http://kurzlink.de/TVVIlA9to zu 2.8) http://kurzlink.de/XEe2zHfDy
	3. **De**zentrale **Suchmaschinen** 3.1 Problematik **anonymisierender** Suchmaschinen → „Heuchelei“? 3.2 Idee einer **dezentralen** Suchmaschine am Bsp. **YaCy** PRO → Suchanfragen verlassen den eigenen	Lehrervortrag	- Namen und Links zweiter Beamer: zu 3.1)https://duckduckgo.com/ https://metager.de/ https://startpage.com/ zu 3.2) http://yacy.de/

	Rechner *nicht* → mitbestimmen, was im Index ist → Einflussnahme auf die Wertigkeit von Suchergebnissen CON → man muss YaCy erst einmal installieren → Index hat aktuell nicht die Größe etablierter Suchmaschinen 3.2.1 YaCy-Suche am Bsp.: → HU-Berlin → Friedrich Schorlemmer 3.2.2 YaCy-Administrationszugang Für Sprache: → Erste Schritte / Anwendungsfall & Zugangsdaten Für allgemeine Systeminformationen: → Überwachung / Systemstatus → Überwachung / Peer-to-Peer Netzwerk 3.2.3 YaCy-Indexierung Crawlen starten: → Erste Schritte / Webseiten laden mit Crawler Crawlvorgang überwachen: → Überwachung / Crawler Überwachung → Überwachung / Crawler Überwachung / Warteschlangen / Lokal → Überwachung / Crawler Überwachung / Crawl Results / Lokales Crawlen bis **20:00** (10min)		zu 3.2.1) http://localhost:8090/ http://www.friedrich-schorlemmer.de/
	4. Exkursion mit dem **Tor-Browser** 4.1 Erklärung und „**Belehrung“** sowie Unterschied **visible/insivisble Web**, **Surface Web**, **Darknet** und **Deep Web** PRO Umgehung von Zensur, Anonymisierung CON Anonymisierung illeg. Machenschaften 4.1.0 Anwendungsmöglichkeiten also: 4.1.1 anonymisierter Seitenabruf 4.1.2 Zugang zu **hidden services**/Deep Web 4.2 **Tor Browser Bundle** installieren 4.3 **IP -Vergleich** mit myip.is 4.4 eine .onion-Seite **finden** am Bsp. **wikipedia.org/wiki/The_Hidden_Wiki**	Lehrervortrag	- Namen und Links zweiter Beamer: zu 4.1) http://kurzlink.de/CBUvNC5YW zu 4.2) https://www.torproject.org/ zu 4.3) http://myip.is/ zu 4.4) https://de.wikipedia.org/wiki/The_Hidden_

	4.5 eine .onion-Seite **abfrufen** am Bsp. **duckduckgo.com** bis **20:10** (10min)		Wiki zu 4.5) https://duckduckgo.com/ Tor: http://jh32yv5zgayyyts3.onion/
	Puffer 1: Verweis auf **prism-break.org** → sicher(re)e Alternativen zu gängigen Anwendungen bis **max. 20:10**	Lehrervortrag	- Namen und Links zweiter Beamer: https://prism-break.org/
	Puffer 2: Verweis auf **privacygrade.org** bis **max. 20:10**	Lehrervortrag	- Namen und Links zweiter Beamer: http://privacygrade.org/
	Puffer 3: Verweis auf **alternative E-Mailanbieter** wie **mailbox.org**, **mykolab.com** oder **posteo.de**, in Verbindung mit **Thunderbird** bis **max. 20:10**	Lehrervortrag	- Namen und Links zweiter Beamer: https://mailbox.org/ https://mykolab.com/ https://posteo.de/ https://www.mozilla.org/de/thunderbird/
	Puffer 4: Alternative **ROMs** für Smartphones am Bsp. **cyanogenmod.org** bis **max. 20:10**	Lehrervortrag	- Namen und Links zweiter Beamer: http://www.cyanogenmod.org/
20:10-20:20 (10min) **Pause**	Hinweis für Getränkeautomat und Toiletten	**Pause**	
20:20-20:50 (30min) **Praxis1**	- Hinweis: Praxis-Teil einzeln oder in Gruppenarbeit - Hinweis: bei Fragen immer fragen **Möglichkeit 1**: keine Aufgaben, genannte Möglichkeiten selbst ausprobieren **Möglichkeit 2**: Aufgaben: 1. Überprüfen Sie ihre **Passwörter** in Bezug auf Komplexität mit http://www.passwordmeter.com/ ! 2. Vergleichen Sie die Funktionalität ihrer favorisierten Webseiten per **Firefox und NoScript** ohne und mit deaktivierten Java Script-Funktionen – forschen Sie nach, welche Dienstleister sich hinter den blockierten Seiten verbergen! z. B. http://www.focus.de/ 3. Suchen Sie ihre favorisierten Webseiten über **YaCy** und nehmen Sie sie ggf. in Ihren	Einzel- oder Gruppenarbeit	- präsent sein - Einzelfragen für Reflexionsteil sammeln Links für Aufgaben nach Reihenfolge: zu 1.) http://www.passwordmeter.com/ zu 2.) http://www.focus.de/

	Index auf, falls die Suche keine Ergebnisse liefert! 4. Vergleichen Sie ihre **IP-Adresse** mittels http://myip.is/ mit und ohne Tor-Browser und besuchen Sie ihre favorisierten Webseiten über den **Tor-Browser**! 5. Auf eigene Verantwortung: Machen Sie eine Exkursion ins **Deep Web** mit dem Tor-Browser! Kleine Starthilfe: https://de.wikipedia.org/wiki/The_Hidden_Wiki		zu 4.) http://myip.is/ zu 5.) https://de.wikipedia.org/wiki/The_Hidden_Wiki
20:50-21:00 (10min) **Reflexion**	1. Ersteindruck in Bezug auf die demonstrierten Möglichkeiten erfragen 2. gesammelte Fragen klären	Lehrer-Schüler-Gespräch	- Stichwortsammlung ev. an die Tafel
21:00-21:20 (20min) **Praxis2**	1. Zeit, um weiteres Aufgaben auszuprobieren 2. Animation von **myshadow.org** zeigen 3. Den eigenen digitalen Schatten verfolgen mit **myshadow.org**	Einzel- oder Gruppenarbeit	zu 2.) https://myshadow.org/visualisations/animation zu 3.) https://myshadow.org/
21:20-21:30 (10min) **Abschluss**	Gedanken zur Datenhoheit: 1. **Rechtfertigungssituation**, Trilemma als Argumentationsgrundlage: komfortabel kostenlos datenschonend -> max. zwei Eigenschaften bekommt man 2. **Vorbild** im Umgang digitaler Medien sein 3. **Konsequenz** auch in unbequemen Situationen 4. Weiterbilden, geht auch unkompliziert(er) z.B. mit **sempervideo.de** 5. Bitte um **Kritik** und ggf. **Empfehlung**	Lehrervortrag	

Linkverzeichnis

URL (alphabetisch n. Anfangsbuchstaben der Domainnamen, z. B. https://www.facebook.com/)	Kurz-Link
http://cookiepedia.co.uk/	
http://www.cyanogenmod.org/	
http://distrowatch.com/	
https://duckduckgo.com/ Tor: http://jh32yv5zgayyyts3.onion/	
https://www.eff.org/https-everywhere	
http://www.keepass.info/	

http://www.linuxmint.com/	
http://masterpasswordapp.com/	
https://metager.de/	
https://www.mozilla.org/de/thunderbird/	
https://addons.mozilla.org/de/firefox/addon/adblock-edge/	http://kurzlink.de/KZPGXT4kI
https://addons.mozilla.org/de/firefox/addon/anonymox/	http://kurzlink.de/OgDMc1Csa
https://addons.mozilla.org/de/firefox/addon/canvasblocker/	http://kurzlink.de/LhRbpqP41
https://addons.mozilla.org/de/firefox/addon/flagfox/	http://kurzlink.de/hKcboB2fh
https://addons.mozilla.org/de/firefox/addon/noscript/ (Vgl. https://www.youtube.com/watch?v=ybzP0oftI4c)	http://kurzlink.de/BzUyxE2U2 (Vgl. http://kurzlink.de/A9nA6JOOa)
https://addons.mozilla.org/de/firefox/addon/self-destructing-cookies/	http://kurzlink.de/TVVIlA9to
https://addons.mozilla.org/de/firefox/addon/wot-safe-browsing-tool/ (Vgl. https://www.youtube.com/watch?v=4HJ87iNkgX4)	http://kurzlink.de/gJQrobZ4m (Vgl. http://kurzlink.de/ySLrwC3Tj)
https://mailbox.org/	
http://myip.is/	
https://mykolab.com/	
https://myshadow.org/ → https://myshadow.org/visualisations/animation	
http://www.passwordmeter.com/	
https://posteo.de/	
https://prism-break.org/	
http://privacygrade.org/	
http://www.sempervideo.de/	
https://startpage.com/	
https://www.torproject.org/	
http://yacy.de/	
http://www.zeit.de/zeit-magazin/essen-trinken/2014-11/baeckerei-brot-backen-handwerk-deutschland-karte	http://kurzlink.de/3NLnhu1Mx

Hinweis: Internetseiten von Tracking-Diensten aus dem Abschnitt 2.6 (NoScript) sind nicht aufgeführt.

Literaturhinweise

SCHMIDT, J.: „Eines für alle – Ein neues Konzept für den Umgang mit Passwörtern“, Magazin für Computertechnik c't 2014, Heft 18, 82, online abrufbar unter: http://www.heise.de/ct/ausgabe/2014-18-Ein-neues-Konzept-fuer-den-Umgang-mit-Passwoertern-2284364.html – Kurzlink: http://heise.de/-2284364 (zuletzt aufgerufen: 17. Jan 2015).

SCHMIDT, J.: „Passwort-Schutz für jeden - Sicherheit mit System und trotzdem unberechenbar“, Magazin für Computertechnik c't 2013, Heft 3, 88, online abrufbar unter: http://www.heise.de/ct/ausgabe/2013-3-Sicherheit-mit-System-und-trotzdem-unberechenbar-2330349.html – Kurzlink: http://heise.de/-2330349 (zuletzt aufgerufen: 17. Jan 2015).

STORM, I. T.: „31C3: Kinderpornografie im Tor-Netzwerk stark nachgefragt“, heise.de, 31.12.2014, online abrufbar unter:
http://www.heise.de/newsticker/meldung/31C3-Kinderpornografie-im-Tor-Netzwerk-stark-nachgefragt-2507444.html
(http://kurzlink.de/CBUvNC5YW (zuletzt aufgerufen: 18. Jan 2015).

Weinberg, G.: „DuckDuckGo now operates a Tor exit enclave“, gabrielweinberg.com, 13. Aug 2010, http://www.gabrielweinberg.com/blog/2010/08/duckduckgo-now-operates-a-tor-exit-enclave.html – Kurzlink: http://kurzlink.de/hTwy9skPM (zuletzt aufgerufen: 18. Jan 2015).

WIKIPEDIA.DE: Art. „The Hidden Wiki“, https://de.wikipedia.org/wiki/The_Hidden_Wiki (zuletzt aufgerufen: 18. Jan 2015).

Informeller Ideenkatalog zum Umgang mit der globalen Überwachungsaffäre

Ideen, Vorschläge und Empfehlungen zur Umsetzung für die HU-Berlin, initiiert durch die stud. Initiative "Jahr 1 nach Snowden"

Initiator und Kontakt: roland.hummel@student.hu-berlin.de (Student, Theol. Fak., HU-Berlin; keyID: 0x5A22CEFB – S/MIME-Zertifikat: 6368458645442538)

Der Wunsch nach einem "Ideenkatalog" und den daraus entwickelten, hier vorgestellten Ideen, entstand im Verlauf der stud. Initiative „Jahr 1 nach Snowden“, ohne eine Beauftragung durch die HU Berlin. Der Ideenkatalog ist ein Ergebnis der Arbeit der Initiative.

Die Ideen sollen als *informeller* Impulsgeber für techn. Lösungen dienen, Überwachung staatlicher wie auch wirtschaftlicher Institutionen zum Schutz der HU-Berlin frühzeitig zu erkennen und zu identifizieren, um einerseits erneute Fälle konkreter Überwachung wissenschaftlicher Mitarbeiter_innen wie Andrej Holm im Jahr 2007 zu verhindern und andererseits das verdachtsunabhängige Sammeln von E-Maildaten, Daten zum Surfverhalten, Daten von Forschungsprojekten sowie personenbezogene Verwaltungsdaten präventiv abzuwenden.

Das Anliegen verfolgend, den Ideenkatalog nicht an der Realität vorbei und als möglichst gemeinschaftliches Projekt zu erstellen, luden die stud. Initiatoren am 28. Okt. 2015 die HU-DV-Beauftragen, die HU-Datenschutzbeauftragten sowie die Vertreter_innen des HU-ReferentInnenrates (Politisches Mandat und Datenschutz) zu einem persönlichen Treffen ein, um den Entwurf des Ideenkataloges zu diskutieren. An der Diskussion beteiligten sich zwölf DV-Beauftragte.

Durch die engagierte Mitarbeit der anwesenden DV-Beauftragten, für die sich die stud. Initiatoren an dieser Stelle noch einmal herzlich bedanken möchten, wurde der Ideenkatalog auf einen Stand gebracht, der als nach wie vor informeller, aber fundierter Impulsgeber die verantwortlichen Instanzen der HU-Berlin darin unterstützen möchte, über die Problematik von staatlicher und wirtschaftlicher Überwachung aufzuklären und dieser adäquat zu begegnen.

Dieser Sammelband führt den Stand vom 28. Okt. 2015, die aktuelle Fassung wird als Teil des HU-Wikis unter folgender Adresse gepflegt: https://wikis.hu-berlin.de/dvb/Jahr1nachSnowden-Ideenkatalog

Motivation:

0.1 Die IT als „5. Macht im Staat“ trägt Verantwortung für die Verwendung der von ihr bereitgestellten Infrastrukturen, nachdem die Snowden-Enthüllungen den Missbrauch derselben verdeutlichten (Michael Hayden: „We kill people based on metadata.“).

0.2 Die IT hat durch Konzeption von IT-Infrastrukturen einen maßgeblichen Einfluss auf den Datenschutz der Nutzer_innen und sollte entsprechend den mündigen Umgang mit dem digitalen Raum nicht nur fordern, sondern unter den besonderen Gegebenheiten der Überwachung über etablierte Standards hinaus ermöglichen und fördern.

1. Vermittlung von Kompetenzen zur Schulung von praktischer Kompetenz zum Umgang mit Überwachung durch **regelmäßige CMS-Workshops**:

Die Praxisveranstaltungen der Jahr 1 nach Snowden-Initiative zeigten eine dauerhaft hohe Teilnahme an den Veranstaltungen "Rollentausch: (sich) selbst überwachen!", "Einführung in verschlüsselte Kommunikation" sowie "Datenhoheit und Datenkontrolle ohne Verschlüsselungstechniken" (http://jahr1nachsnowden.de/veranstaltungen). Die Initiative hat Veranstaltungskonzepte erarbeitet, die als Grundlage für zukünftige Veranstaltungen dieser Art dienen können (abrufbar unter oben genanntem Link).

Zielführend für das Vorhaben wäre die Kooperation mit den Kryptographie-Workshops der jur. Fakultät sowie die regelmäßige Forführung von CMS-Workshops zur E-Mailverschlüsselung mittels der vom CMS bereitgestellten S/MIME-Zertifikate.

2. Absicherung der öffentlichen Computerarbeitsplätze für eine überwachungsfreie(re) Forschung:

Bereits erfolgte Überwachungsskandale eines Mitarbeiters der HU (Andrej Holm, 2007) zeigen den Bedarf an Schutzmaßnahmen für eine überwachungsfreie(re) Forschung. Dienlich wären diesem Anliegen:

2.1 Tor-Unterstützung durch die HU-Berlin zum Schutz wissenschaftlicher Recherchen sowie der Ermöglichung eines anonymen Zugangs zu Wissen auch über Zensurgrenzen hinweg (https://www.torproject.org/). Aktuelle Einsatzszenarien zur Nutzung von Tor sind:

2.1.1 Client (ein wenig overhead traffic, simpelste Lösung ohne akt. Beitrag zum Tor-Netzwerk)
2.1.2 Relay (konfigurierbarer overhead traffic, juristisch irrelevant)
2.1.3 Relay+Directory (konfigurierbarer overhead traffic, juristisch irrelevant)
2.1.4 Exit relay (konfigurierbarer overhead traffic, juristisch relevant)
2.1.5 Exit relay+Directory (konfigurierbarer overhead traffic, juristisch relevant)

Förderlich für dieses Unterfangen sind zum einen die realistische Einschätzung der aktuellen Situation des Tor-Netzwerkes (Anzahl kompromittierter Tor relays) sowie zum anderen eine Konzeption von Projekten, die eine Installation von Tor unter den Schutz der Forschungsfreiheit stellen.

2.2 Absicherung/Erweiterung von Browsern mit Add-ons und alternativen Suchmaschinen

2.2.1.1 **Suchmaschinenersatz** zu Google&Co, bspw. durch Angebot einer eigenen Sichmaschine betrieben durch die HU, mögliche Varianten: https://searx.me/about eher als http://yacy.de/, diesbzgl. Idee eines Portals *find.cms.hu-berlin.de*.

2.2.1.2 Voreinstellung einer **anonymisierenden Metasuchmaschine** in den installierten Browsern bei allen neu einzurichtenden HU-Computerarbeitsplätzen, Server-Profilen der öffentlichen Computerarbeitsplätze und Empfehlungen für die Nutzer_innen bestehende Arbeitsplätze, https://ixquick.com/, https://startpage.com/, https://duckduckgo.com/ anstelle der voreingestellten Suchmaschine Google bzw. Bing ("opt-in" in Bezug auf Google&Co statt wie aktuell "opt-out").

2.2.2 Absicherung der **Browser mit vorinstallierten Add-ons**, die Nutzer_innen möglichst wenig einschränken, jedoch sicherheitsrelevante Einblicke „hinter die Kulissen“ des WWW ermöglichen, Beispiele:

2.2.2.1 Ghostery („passiv“) in Bezug auf Usability eher als NoScript (ev. nach Aufklärung über Funktionsweise, da hier aktives Eingreifen erforderlich); zu beachten sei jedoch die Problematik: https://de.wikipedia.org/wiki/Ghostery#Kritik

2.2.2.2 HTTPS Everywhere der Electronic Frontier Foundation (fordert https wann immer möglich)

2.2.2.3 Flagfox (in welchem Land/Datenschutzrecht wird die aufgerufene Seite gehostet)

2.2.2.4 Self-Desctructing Cookies (Cookies löschen beim Verlassen der Seite)

2.3 Fokus Open Source Software

2.3.1 Obgleich Open Source Software nicht prinzipiell sicherer ist als Closed Source Software, bietet doch Open Source gegenüber Closed Source eine weitaus bessere Möglichkeit der Prüfung auf Backdoors und Sicherheitslücken. Zudem erschafft Closed Source Software Hürden und Kompatiblitaetsprobleme für Nutzer_innen, welche aus finanz. Gründen keinen Zugang zu Closed Source-Programmen haben. Aus diesem Grund sollte Open Source zumindest in gleichrangiger Art und Weise für Endanwender_innen angeboten werden, wo entsprechende **Open Source Pendants** zu Closed Source Software existieren (bspw. LibreOffice neben Microsoft Office, Thunderbird neben Outlook).

2.3.2 Templates/Vorlagen der HU sollten entsprechend ebenso für Open Source Formate bereitgestellt werden (bspw. Briefköpfe im ODT-Format). Die Entkoppelung von proprietären Formaten hin zu **quelloffene**n **Standards** sichert zudem die langfristige Nutzbarkeit von digitalen Erzeugnissen aller Art.

2.3.3 Der Punkt „**Linux** als alternatives Betriebssystem für Computerarbeitsplätze“ steht in diesem Zusammenhang, erfordert aber eine gesonderte Auseinandersetzung. Die ursprüngliche Bitte der „Jahr 1 nach Snowden“-Initiatoren bestand darin, zumindest an öffentlichen Computerarbeitsplätze Linux als alternative zur Windows-Anmeldung anzubieten, unabhängig von einer Bedarfsermittlung. Das Anliegen wurde von den DV-Beautragen freundlich zur Kenntniss genommen, überfordert aktuelle Kapazitäten allerdings in besonderem Maße und muss daher gesondert behandelt werden.

2.4 Empfehlung zur Nutzung des **HU-eigenen DatenCloud-Dienstes** https://box.hu-berlin.de/, sobald dessen Testphase abgeschlossen ist. Falls personenbezogene Daten bzw. sensible Forschungsdaten in einer Cloud gespeichert werden müssen, wäre ein **Präsidiumsbeschluss** wünschenswert, der zur Nutzung der HU-DatenCloud in diesem Zusammenhang verpflichtet.

3. Allg. **Regelung** an die Abteilungen der HU, bei Verwendung **kommerzieller sozialer Netzwerke**, deren Geschäftsmodell auf der Verwertung von Nutzer_innendaten liegen, nicht aktiv zu bewerben (bspw. „Facebook-Buttons“ auf den Seiten der HU) und von entsprechenden Seiten besagter sozialer Netzwerke nur *heraus* zu verweisen, nicht aber von den Seiten der HU hin zu diesen Netzwerken.

4. E-Mailverschlüsselung

4.1 **Automatische Ausstellung von S/MIME-Zertifikaten** für bereits vorhandenes, gut funktionierendes, aber kaum genutztes System zur E-Mailverschlüsselung (https://www.cms.hu-berlin.de/de/dl/zertifizierung) für alle **Neuanstellungen** an der HU (Idee eines langfristigen Schneeballeffektes zur Nutzung dieses Systems + „opt-out“ statt wie aktuell „opt-in“). Zu diesem Zweck soll die Erstellung von Softwarezertifikaten automatisch im Antrag eines CMS-Accounts inbegriffen sein (akt. muss dies gesondert beantragt werden, die CMS-Seite überfordert mit einer Vielzahl an „Technizismen“, deren Zusammenhang sich Endanweder_innen schwer erschließt und daher die Eigeniinitiative für einen entsprechenden Antrag hemmt). Ein Hinweis in Begrüßungsformularen soll darüber informieren, dass darüber hinaus die Erstellung einer Smartcard als „Hardwarezertifikat“ möglich ist (erfordert ev. nicht überall vorhandene Chipkartenleser). DV-Beauftragte helfen entsprechend bei der Einführung in die Nutzung des Verfahrens und klären über den unsicheren E-Mailstandard auf.

4.2 Ein **Präsidiumsbeschluss** möge die **obligatorische Verschlüsselung** von E-Mails mit **personenbezogenen Daten** beschließen, da sich sonst die Verwendung eines sicheren E-Mailtransportes nicht durchsetzt.

5. Würdigung von Edward Snowden für seine beispiellose Aufklärungsarbeit als einen Dienst an der gesamten Menschheit. Erste Ideen: „Edward Snowden-Hörsaal“, „Edward Snowden-Computerpool“, „Treppenstufen-Kunstprojekt“ zu Überwachungsprogrammen Prism / Tempora / Fashiocleft / XkeyScore etc (analog „Vorsicht Stufe“ im HU-Hauptgebäude).

6. (mit den Anwesenden aus Zeitmangel nicht diskutiert:) Keine weitere Unterstützung der **Lobbyarbeit** datenschutzproblematischer Firmen für Initiativen wie "Get Office free from your school" durch die HU.

7. Langfristige Umsetzung des Ideenkatalogs

7.1 Da die **Umsetzung und Koordination** zum Ausbau der IT-Sicherheit sich über einen langen Zeitraum erstrecken wird, zeichnet sich ab, dass eine sinnvolle Umsetzung nur durch Schaffung zusätzlicher personeller Kapazitäten zu erreichen ist. Konkret sollte die Position einer/s **IT-Sicherheitsbeauftragten** eingerichtet werden.

7.2 Das Thema „IT-Sicherheit“ und „Überwachungsschutz“ sollte, sofern noch nicht vorhanden, fester Bestandteil von **DV-Konzeptionen** sein, um langfristig die Sensibilisierung für das Thema auch innerhalb des CMS aufrecht zu erhalten.

Anhänge

1. „Vom Sinn des Privaten“ – Präsentationsfolien der Eröffnung
2. „Vom Sinn des Privaten“ – Präsentationsfolien von Florian Wobser und Tom Gehrke
3. „Vom Sinn des Privaten“ – Literatur- und Medienempfehlungen von Florian Wobser und Tom Gehrke
4. „Vom Sinn der Kryptographie“ – Präsentationsfolien der Eröffnung
5. „Vom Sinn der Überwachung“ – Präsentationsfolien der Veranstaltung
6. „Rollentausch: (sich) selbst überwachen!“ – Präsentationsfolien der Praxisveranstaltung 1
7. „Einführung in verschlüsselte Kommunikation“ – Präsentationsfolien der Praxisveranstaltung 2
8. „Datenhoheit und Datenkontrolle“ – Präsentationsfolien der Praxisveranstaltung 3

Wir bitten zu entschuldigen, dass wir keine Seitennummerierung in den Anhängen vorgenommen haben. Zur Orientierung in den Anhängen achten Sie bitte auf die Beschriftungen in den Fußzeilen sowie auf die Nummerierung der Folien.

Aufgrund der Verkleinerung der Originalfolien auf ca. 25% der ursprl. Größe sind einige Bildunterschrifen und Quellennachweise der Originale nicht mehr lesbar. Davon betroffene Textstellen wurden in der Form [Anm.: ...] den jew. Folien neu hinzugefügt. Die Folien finden Sie in digitaler Form zum Download auf der Projektseite bzw. im Moodle-Kurs der Initiative (s. Abschnitt „Allgemeine Hinweise“).

Folie 1

Vom Sinn des Privaten

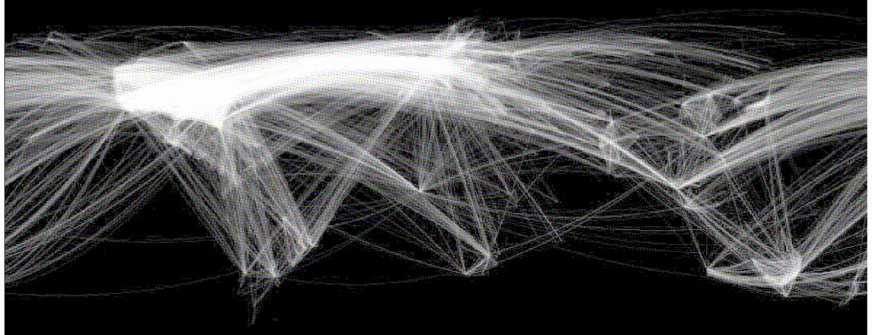
www.Jahr1nachSnowden.de

Auftaktveranstaltung

Herzlich willkommen!

Initiatoren: Amon Kaufmann und Roland Hummel

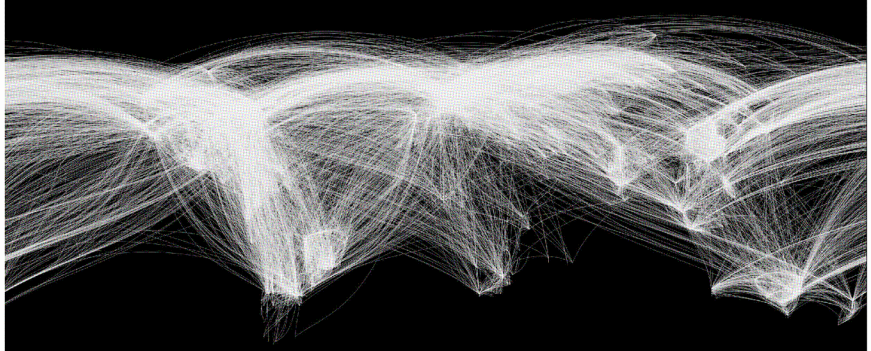
Folie 2



2007

© ChrisHarrison.net

Folie 3



2011

© ChrisHarrison.net

Folie 4

Bild: Teufelsberg Berlin 2013 © R. Hummel

Anhang 1

„Vom Sinn des Privaten“ - Präsentationsfolien der Eröffnung

Folie 5

Bild: „Freiheit statt Angst“-Demo Berlin 2014 © R. Hummel

Folie 6

Gesellschaft

„nichts enthüllt“ (FAZ)

Ohnmacht

„Niveau von digitalen Analphabeten“ (DRadio)

Folie 7

Gastredner_innen

Michaela Zinke
Tom Gehrke
Florian Wobser

Folie 1

VOM SINN DES PRIVATEN

[!!! COPYRIGHT ;-) DIESER PRÄSENTATION BEI:]

T. Gehrke
F. Wobser
(Universität Rostock)

Theologische Fakultät – Humboldt Universität – Berlin 03/11/14

www.jahr1nachsnowden.de

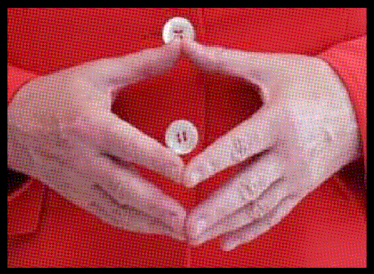
Folie 2

Gliederung

1) Vom heutigen Unsinn des Nicht-Privaten
2) Vom einstigen Sinn des Öffentlichen
3) Vom Unsinn des Nicht-Öffentlichen
4) Vom Un/Sinn des Öffentlichen / Privaten

Folie 3

1) Vom heutigen Unsinn des Nicht-Privaten



http://blogs.taz.de/drogerie/files/2014/02/Merkel_Raute-624x312.jpg

...in post-demokratischen Zeiten...

[Anm.: Bildnachweis: http://blogs.taz.de/drogerie/files/2014/02/Merkel_Raute-624x312.jpg]

Folie 4

1) Vom heutigen Unsinn des Nicht-Privaten

»Transparenz«

Unfreiheit Freiheit

Widerstand

Folie 5

1) Vom heutigen Unsinn des Nicht-Privaten

»Transparenz«

Unfreiheit ? Freiheit

Widerstand

Folie 6

1) Vom heutigen Unsinn des Nicht-Privaten

»Transparenz« des Privaten ↔ »Transparenz« des Öffentlichen

↓ ! ↑

Unfreiheit ↔ Widerstand

✦

Folie 7

1) Vom heutigen Unsinn des Nicht-Privaten

»Transparenz« des Privaten ↔ »Transparenz« des Öffentlichen

↓ ! ↑

Unfreiheit ↔ Widerstand

✦ Freiheit ?

Folie 8

[Anm.: Videonachweis: http://www.dctp.tv/filme/edd-transparenz/]

Jacob Applebaum; Christoph Bieber (Tagung „Einbruch der Dunkelheit" – Berlin – Januar 2014)
http://www.dctp.tv/filme/edd-transparenz/ [Auszug; zum Kontext vgl. speziell 0:32:00 bis 0:52:00]

Anhang 2

„Vom Sinn des Privaten" - Präsentationsfolien von Florian Wobser und Tom Gehrke

Folie 9

Folie 10

2) Vom einstigen Sinn des Öffentlichen

I. Kant:

C

Freiheit durch
Autonomie – Publizität – Moralität

D

Trennung zwischen einem
»öffentlichen« & »privaten« Vernunftgebrauch

Folie 11

2) Vom einstigen Sinn des Öffentlichen

I. Kant:

„[…] der *öffentliche* Gebrauch seiner Vernunft muß jederzeit frei sein, und der allein kann Aufklärung unter Menschen zustande bringen; der *Privatgebrauch* derselben aber darf öfters sehr enge eingeschränkt sein, ohne doch darum den Fortschritt der Aufklärung sonderlich zu hindern. Ich verstehe aber unter dem öffentlichen Gebrauche seiner eigenen Vernunft denjenigen, den jemand *als Gelehrter* von ihr vor vor dem ganzen Publikum der *Leserwelt* macht. Den Privatgebrauch nenne ich denjenigen, den er in einem gewissen ihm anvertrauten *bürgerlichen Posten* oder Amte von seiner Vernunft machen darf."

Beantwortung der Frage: Was ist Aufklärung? (1783)

Folie 12

2) Vom einstigen Sinn des Öffentlichen

J. Habermas:

C

Emanzipation durch
kommunikatives Handeln – Diskurs – Ethik

D

juridisch-demokratische Konsensorientierung
ignoriert Konflikt »System« vs. »Lebenswelt«

Folie 13

2) Vom einstigen Sinn des Öffentlichen

J. Habermas:

„[…] Voraussetzungen einer politisch fungierenden Öffentlichkeit: die objektiv mögliche Minimalisierung der bürokratischen Dezisionen und eine Relativierung der strukturellen Interessenkonflikte nach Maßgabe eines erkennbaren Allgemeininteresses – diesen Voraussetzungen läßt sich heute nicht mehr schlechthin ein utopischer Charakter vindizieren. Die Dimension der Demokratisierung sozialstaatlich verfaßter Industriegesellschaften ist nicht von vornherein limitiert durch eine […] erwiesene Undurchdringlichkeit und Unauflösbarkeit der irrationalen Beziehungen sozialer Macht und politischer Herrschaft. Der Streit einer kritischen Publizität mit der zu manipulativen Zwecken bloß veranstalteten ist offen."

Strukturwandel der Öffentlichkeit (1962)

Folie 14

Folie 15

3) Vom Unsinn des Nicht-Öffentlichen

Kritiker dieses klassischen Aufklärungs- & Öffentlichkeitsbegriffs

Folie 16

3) Vom Unsinn des Nicht-Öffentlichen

G.W.F. Hegel:

C

dialektisches Überschreiten der Trennung des »öffentlichen« & »privaten« Vernunftgebrauchs

D

die gesetzgebende Gewalt & Souveränität des Staates als das Prinzip der Sittlichkeit

Folie 17

3) Vom Unsinn des Nicht-Öffentlichen

G.W.F. Hegel:

„Was vernünftig ist, das ist wirklich; und was wirklich ist, das ist vernünftig."

Grundlinien der Philosophie des Rechts (1821)

[Anm.: Bildunterschrift: NSA Headquarter (Fort Meade, Maryland US) GCHQ (Cheltenham, Gloucestershire UK]

[Motto: »It's all absolutely legal (– if it's not, who cares, stupid?)!«]

[Anm.: Quellenangaben:
http://images.politico.com/global/2013/06/10/130610_nsa_building_ap_3281.jpg
http://www.digitaljournal.com/img/3/6/3/9/8/8/i/1/5/0/o/GCHQ-aerial.jpg]

Folie 18

3) Vom Unsinn des Nicht-Öffentlichen

K. Marx & F. Engels:

C

materialistische Analyse des souveränen Staats; Kritik der politischen Ökonomie

D

[… Bibliotheken über Bibliotheken… ;-)]

Folie 19

3) Vom Unsinn des Nicht-Öffentlichen

K. Marx & F. Engels:

„Das Bedürfnis nach einem stets ausgedehnteren Absatz für ihre Produkte jagt die Bourgeoisie über die ganze Erdkugel. Überall muß sie sich einnisten, überall anbauen, überall Verbindungen herstellen."

Manifest der Kommunistischen Partei (1848)

»Privacy is no longer a social norm.«

[Anm.: Bildunterschrift: Mark Zuckerberg (Gründer von Facebook)
Quellenangabe: http://www.theguardian.com/technology/2010/jan/11/facebook-privacy]

Folie 20

[Anm.: Videonachweis: http://www.youtube.com/watch?v=UPltW8wg6aI]

Sarah Harrison; Alexa O'Brien (Tagung „re:publica" – Berlin – Mai 2014)
http://www.youtube.com/watch?v=UPltW8wg6aI [Auszug; vgl. speziell 0:46:20 bis 0:50:30]

Folie 21

Folie 22

3) Vom Unsinn des Nicht-Öffentlichen

M. Foucault:

„Macht ist nicht eine Institution, ist nicht eine Strategie, ist nicht eine Mächtigkeit einiger Mächtiger. Die Macht ist der Name, den man einer komplexen strategischen Situation in einer Gesellschaft gibt."

Der Wille zum Wissen. Sexualität und Wahrheit 1 (1976)

Folie 23

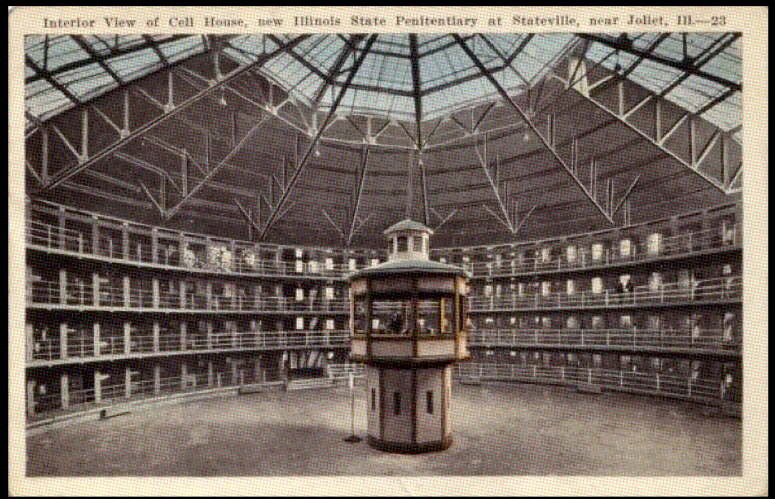
3) Vom Unsinn des Nicht-Öffentlichen

M. Foucault:

- **»Mikrophysik der Macht« & Selbsttechnologien**
- **Pastoral – Biopolitik – Gouvernementalität**
- **Disziplinargesellschaft**
  u.a. das »Panopticon« als ein Dispositiv

Folie 24

3) Vom Unsinn des Nicht-Öffentlichen



[Anm.: Bildüberschrift: "Interior View of Cell House, new Illinois State Penitentiary at Stateville, near Joliet, I11.-23"
Bildnachweis: http://www.e-ir.info/wp-content/uploads/Panopticon.jpg]

Folie 25

3) Vom Unsinn des Nicht-Öffentlichen

G. Deleuze & F. Guattari:

- **»Kriegsmaschinen« vs. Kapitalismus & Staat**
- **subversiv-heimliche »Mikropolitiken«**
- **Kontrollgesellschaft**
  u.a. »Auto-Surveillance« als eine Konsequenz

Folie 26

3) Vom Unsinn des Nicht-Öffentlichen

G. Deleuze & F. Guattari:

„Foucault gilt nicht selten als Denker der Disziplinargesellschaften […]. Aber in Wirklichkeit gehört er zu den ersten, die sagen, daß wir dabei sind, die Disziplinargesellschaften zu verlassen […]. Wir treten ein in Kontrollgesellschaften, die nicht mehr durch Internierung funktionieren, sondern durch unablässige Kontrolle und unmittelbare Kommunikation. […] Jeden Gesellschaftstyp kann man selbstverständlich mit einem Maschinentyp in Beziehung setzen: […] energetische Maschinen für die Disziplinargesellschaft, Kybernetik und Computer für die Kontrollgesellschaften."

Postskriptum über die Kontrollgesellschaften (1990)

Folie 27

[Anm.: Videonachweis: http://www.dctp.tv/#/filme/rp14-deibert/]

Ron Deibert; Philipp Banse (Tagung „re:publica" – Berlin – Mai 2014)
http://www.dctp.tv/#/filme/rp14-deibert/ [Auszug; vgl. zum Kontext speziell 0:12:00 bis 0:19:00]

Folie 28

Folie 29

[Anm.: Bildnachweise: http://www.longwoodfl.org/images/Police/09.01.2011%20FDLE%20See%20Something%20Say%20Something_Digital%20Poster_840x400.jpg
http://images.rapgenius.com/83eab67bfe7e9e2ff9e30ec675eb979d.390x328x1.png]

Folie 30

»Nothing to hide!«

Eric Schmidt (CEO Google)

[Anm.: Bildunterschrift: Eric Schmidt (CEO Google)
Bildnachweis: http://p5.focus.de/img/fotos/crop3360836/7372716111-w1200-h627-o-q75-p5/dig-google-eric-schmidt.jpg]

http://p5.focus.de/img/fotos/crop3360836/7372716111-w1200-h627-o-q75-p5/dig-google-eric-schmidt.jpg

Folie 31

3) Vom Unsinn des Nicht-Öffentlichen

G. Deleuze & F. Guattari:

„Ein System wie der Kapitalismus leckt auf allen Seiten, es leckt, und dann dichtet der Kapitalismus die Risse ab, macht Knoten. Sorgt für Verklammerungen, um zu verhindern, daß die Fluchten zu zahlreich werden. […] Doch bislang hat es auf dem revolutionären Feld keine Kriegsmaschine gegeben, die auf ihre Weise nicht auch etwas ganz anderes reproduziert hätte, nämlich einen Staatsapparat, den Organismus der Unterdrückung schlechthin.

Fünf Thesen über die Psychoanalyse (1973)

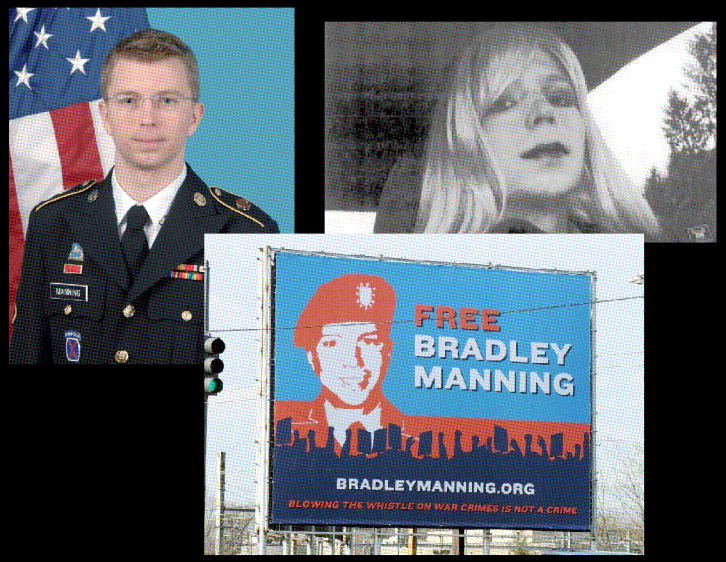
Folie 32

[Anm.: Bildnachweise:
http://i.telegraph.co.uk/multimedia/archive/02311/assange-im-julian_2311882k.jpg
http://static.guim.co.uk/sys-images/Guardian/Pix/pictures/2012/8/24/1345820560841/Julian-Assange-speaks-fro-008.jpg]

Anhang 2

„Vom Sinn des Privaten“ - Präsentationsfolien von Florian Wobser und Tom Gehrke

Folie 33



[Anm.: Bildnachweise:
http://upload.wikimedia.org/wikipedia/commons/5/5d/Bradley_Manning_US_Army.jpg
http://en.wikipedia.org/wiki/Chelsea_Manning]

Folie 34

[Anm.: Bildnachweis:
http://www.berliner-zeitung.de/image/view/2013/6/4/23598558%2c20473210%2chighRes%2c3cmc5438.jpg]

Folie 35

Folie 36

4) Vom Un/Sinn des Öffentlichen / Privaten

Was tun?
Möglichkeiten zum dargestellten Befund aus der Perspektive kritischer Theorie…

Folie 37

4) Vom Un/Sinn des Öffentlichen / Privaten

subversive praktische Strategien

Folie 38

4) Vom Un/Sinn des Öffentlichen / Privaten

subversive praktische Strategien

- **informationelle Technologien:**

  z.B. Open Source, Hacking, Leaking, Kryptographie

Folie 39

4) Vom Un/Sinn des Öffentlichen / Privaten

subversive praktische Strategien

- **informationelle Technologien:**

  z.B. Open Source, Hacking, Leaking, Kryptographie

- **Kunst:**

  z.B. investigative Fotografie, Filme etc.

  - u.a. Trevor Paglen - u.a. Laura Poitras

  »ART AS EVIDENCE«

  vgl. Tagung „transmediale" – Berlin – Jan./Feb. 2014

Folie 40

[Anm.: Videonachweis: http://www.youtube.com/watch?v=SDxue3jGAug]

Trevor Paglen (Tagung „transmediale" – Berlin – Januar/Februar 2014)
http://www.youtube.com/watch?v=SDxue3jGAug [Auszug; vgl. speziell bis 0:01:30 & 0:12:00 bis 0:14:45]

Folie 41

Ai Weiwei

Alcatraz; *jetzt*

[Anm.: Bildnachweise:
http://a57.foxnews.com/global.fncstatic.com/static/managed/img/fn2/travel/876/493/exb6.jpg?ve=1&tl=1
http://clikhear.palmbeachpost.com/wp-content/uploads/2014/09/99841_0051-1280x823.jpg]

Folie 42

4) Vom Un/Sinn des Öffentlichen / Privaten

(unbedingte) Aufklärung & Bildung

Folie 43

4) Vom Un/Sinn des Öffentlichen / Privaten

(unbedingte) Aufklärung & Bildung

- Whistleblowing:

  z.B. Infrastruktur, Rechtsschutz etc.

Folie 44

4) Vom Un/Sinn des Öffentlichen / Privaten

(unbedingte) Aufklärung & Bildung

- Whistleblowing:

  z.B. Infrastruktur, Rechtsschutz etc.

- Ausbildung elementarer Kulturtechniken:

  z.B. informationelle Kompetenzen;
  Medienbildung;
  - ✦ politisch-juridischer Prozess

Folie 45

4) Vom Un/Sinn des Öffentlichen / Privaten

»gemeinsames Dekonstruieren«
sozio-politisch relevanter binärer Kategorien

Folie 46

4) Vom Un/Sinn des Öffentlichen / Privaten

»gemeinsames Dekonstruieren«
sozio-politisch relevanter binärer Kategorien

z.B. J. Derrida: Un / Sinn

X

Öffentliches / Privates

Folie 47

4) Vom Un/Sinn des Öffentlichen / Privaten

»gemeinsames Dekonstruieren«
sozio-politisch relevanter binärer Kategorien

z.B. J. Derrida: Un / Sinn

X

Öffentliches / Privates

✦ Performativität;
auch in juristischer Hinsicht!

Folie 48

4) Vom Un/Sinn des Öffentlichen / Privaten

J. Derrida:

„Doch das Paradoxon, das ich in die Diskussion einbringen möchte, hat folgende Gestalt: Weil sie sich dekonstruieren läßt, sichert die Struktur des Rechts oder – wenn Sie wollen – der Gerechtigkeit, der Justiz als Recht, die Möglichkeit der Dekonstruktion. Wenn es etwas gibt wie die Gerechtigkeit als solche, eine Gerechtigkeit außerhalb oder jenseits des Rechts, so läßt sie sich nicht dekonstruieren. Ebensowenig wie die Dekonstruktion selbst, wenn es so etwas gibt. Die Dekonstruktion ist die Gerechtigkeit."

Gesetzeskraft (1993)

Literatur- und Medienempfehlungen
zum Vortrag *VOM SINN DES PRIVATEN*

Humboldt-Universität
Berlin, 03/11/14
Tom Gehrke & Florian Wobser (Universität Rostock)

Deleuze, Gilles.
- Postskriptum über die Kontrollgesellschaften. In: Unterhandlungen. 1972-1990. Frankfurt am Main, 1993. 254-262.
- Fünf Thesen über die Psychoanalyse. In: Die einsame Insel. Texte und Gespräche von 1953-1974. Hg. D. Lapoujade. Frankfurt am Main, 2003. 398-407.
- Das Aktuelle und das Virtuelle. In: Deleuze und die Künste. Hg. P. Gente und P. Weibel. Frankfurt am Main, 2007. 249-253.

Deleuze, Gilles; Guattari, Félix. Tausend Plateaus. Kapitalismus und Schizophrenie [II]. Berlin, 1997.

Derrida, Jacques.
- Gesetzeskraft. Der »mystische Grund der Autorität«. Frankfurt am Main, 1991.
- Marx' Gespenster. Der Staat der Schuld, die Trauerarbeit und die neue Internationale. Frankfurt am Main, 2004.

Derrida, Jacques; Stiegler, Bernhard. Echographien. Fernsehgespräche. Hg. P. Engelmann. Wien, 2006.

Foucault, Michel.
- Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt am Main, 1977.
- Der Wille zum Wissen. Sexualität und Wahrheit Bd. 1. Frankfurt am Main, 1983.
- Was ist Aufklärung?. In: Ethos der Moderne. Foucaults Kritik der Aufklärung. Hg. E. Erdmann u.a. Frankfurt am Main; New York, 1990. 35-54.
- Was ist Kritik?. Berlin, 1992.
- Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität 1. Frankfurt am Main, 2004.
- Die Geburt der Biopolitik. Geschichte der Gouvernementalität 2. Frankfurt am Main, 2004.

Habermas, Jürgen.
- Theorie des kommunikativen Handelns. Bd. 1. Handlungsrationalität und gesellschaftliche Rationalisierung. Bd. 2. Zur Kritik der funktionalistischen Vernunft. Frankfurt am Main, 1981.
- Moralbewußtsein und kommunikatives Handeln. Frankfurt am Main, 1983.
- Strukturwandel und Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft. Darmstadt; Neuwied, [15]1984.

Hegel, Georg Wilhelm Friedrich. Grundlinien der Philosophie des Rechts oder Naturrecht und Staatswissenschaft im Grundrisse […]. Werke Bd. 7. Frankfurt am Main, [4]1997.

Kant, Immanuel u.a. Was ist Aufklärung? Hg. E. Bahr. Stuttgart, 1996.

Marx, Karl. Zur Kritik der Hegelschen Rechtsphilosophie. Leipzig, 1986.

Marx, Karl; Engels, Friedrich. Manifest der Kommunistischen Partei. Berlin [43]1978.

Vgl. zusätzlich die spannenden vielseitigen und aktuellen „Kontexte" der Links aus unserer Präsentation – u.a. Content zu den Berliner Tagungen „transmediale", „re:publica", „Einbruch der Dunkelheit" etc. oder zum Hamburger „Chaos Communication Congress" 2013...
! Gebündelt findet sich beispielsweise viel Content unter*www.dctp.tv* in der Kategorie *Partner und Events!*

Folie 1

Vom Sinn der Kryptographie

www.Jahr1nachSnowden.de

Ifsamjdi Xjmmlpnnfo!

Initiatoren:
Arnon Kaufmann und Roland Hummel
Moderation:
Roland Hummel

Bildnachweis:
"Internet Map city-to-city connections" © Chris Harrison:
http://www.chrisharrison.net/index.php/Visualizations/InternetMap
(Modifikation mit Genehmigung des Künstlers)

Folie 2

Rückblick

Problem:
Persönliche Betroffenheit!?

Folie 3

Beispiel

Saad Allami

Bildnachweis:
Momentum Group: http://www.momentumsuccess.com/presidents-club.html
Vgl.: „Muslim businessman becomes 'terror suspect' after he texts staff he's going to 'blow away' the competition" (Daily Mail, 04. Feb 2014 - http://kurzlink.de/UxTGoOFX2)

Folie 4

Saad Allami

„Den 24. Januar 2012 wird Saad Allami aus dem kanadischen Quebec nicht so schnell vergessen. Als er gerade seinen siebenjährigen Sohn aus der Schule abholen wollte, fingen ihn Polizeibeamte ab und setzten ihn fest. Anschließend stürmten Ermittler seine Wohnung, durchkämmten die Räume und erklärten seiner Frau, sie sei mit einem Terroristen verheiratet. Arbeitskollegen von ihm wurden parallel dazu während einer Geschäftsreise in die USA an der Grenze abgefangen und mehrere Stunden zu ihren Verbindungen zu Allami befragt.

Was war geschehen?
Saad Allami ist Vertriebsmanager bei einem Telekommunikationsunternehmen – und er ist unbescholtener kanadischer Bürger marokkanischer Abstammung. Drei Tage vor der Festnahme wollte er seine Kollegen motivieren, die sich gerade auf dem Weg zu einer Verkaufsmesse in New York City machten. Allami sendete ihnen eine SMS hinterher, sie mögen mit ihrer Präsentation die Konkurrenz „wegblasen".

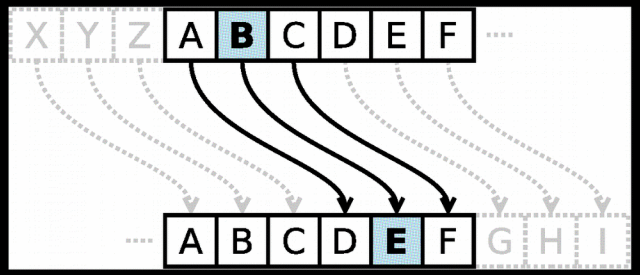
Die kanadische Polizei durchleuchtete den Manager erst nach der Festnahme gewissenhaft und stellte fest, dass der Terrorverdacht haltlos ist. Allami nutzte in seiner SMS das französische Wort „exploser". Die Echtzeit-Analyse des US-amerikanischen Auslandsgeheimdiensts konstruierte offensichtlich aus der marokkanischen Herkunft, der abgefangenen SMS mit dem Begriff „explodieren" und einer Truppe Einreisender als Empfänger der Nachricht eine Terrorwarnung."

Quelle: H. Bleich; „Globaler Abhorwahn - Wie digitale Kommunikation belauscht wird" , In: c't Magazin für Computertechnik 16/2013, S. 112.

Anhang 4
„Vom Sinn der Kryptographie" - Präsentationsfolien der Eröffnung

Folie 5

Kryptographie VS **Rasterfahndung**?



Bildnachweis: „Caesar cipher with a shift of 3", by Cepheus (Own work) [Public domain], via Wikimedia Commons: https://commons.wikimedia.org/wiki/File:Caesar3.svg

Folie 6

Gastredner_innen

Leena Simon

Prof. Dr. Ernst-Günter Giessmann

Folie 7

Zeitplan

19:15-19:25 (10min)	Einführung
19:25-20:15 (50min)	Gastvorträge
20:15-20:25 (10min)	(Denk-)Pause
20:25-21:25 (60min)	Diskussion
21:25-21:30 (5min)	Verabschiedung

Folie 1

Vom Sinn der Überwachung

www.Jahr1nachSnowden.de

Herzlich willkommen!

FJV Berlin

HUMBOLDT-UNIVERSITÄT ZU BERLIN

Initiatoren:
Amon Kaufmann und Roland Hummel
Moderation:
Alexander Czekalla und Roland Hummel

Bildnachweis:
"Internet Map city-to-city connections" © Chris Harrison:
http://www.chrisharrison.net/index.php/Visualizations/InternetMap
(Modifikation mit Genehmigung des Künstlers)

Folie 2

Zeitplan

19:15 - 19:25 (10min) Einführung
19:25 - 19:45 (20min) Thesen der Gastrednerinnen
19:45 - 20:25 (40min) Podiumsdiskussion
20:25 - 20:35 (10min) (Denk-)Pause
20:35 - 21:20 (45min) Offene Diskussion
21:20 - 21:30 (10min) Verabschiedung

Folie 3

Rückblick

1. Vom Sinn der Überwachung
→ **Bedeutung des Privaten**

2. Vom Sinn der Kryptographie
→ **Schutz des Privaten**

Folie 4

Ausblick

3. Vom Sinn der Überwachung
→ **gesellschaftspolitische Dimension der Gefährdung des Privaten**

Anhang 5
„Vom Sinn der Überwachung“ - Präsentationsfolien der Veranstaltung

Folie 5

Ausblick

„[...] anlasslose Massenüberwachung, wie sie Geheimdienste heute ausüben, wirkt auf uns und unsere Demokratien genau wie eine Krankheit. Sie macht uns schwach. Wie ein Virus steckt sie einen nach dem anderen an.“

(Friedemann Karig, Deutschlandfunk, 03.01.2015)

[Anm.: Quelle:
Friedemann Karig: „Staatliche Überwachung - Befallen vom Überwachungsvirus“, Deutschlandfunk, 04.01.2015:
http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639]

Zitat:
Friedemann Karig: „Staatliche Überwachung - Befallen vom Überwachungsvirus“, Deutschlandfunk, 04.01.2015:
http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639

Folie 6

Problem

Visualisierung von Überwachung

Folie 7

[Anm.: Bildnachweis:
„batman-vs-the-joker.jpg“, posted by nDoet: https://mywonderwall.wordpress.com/tag/the-dark-knight/ © Warner Bros. Entertainment Inc.]

Bildnachweis:
„batman-vs-the-joker.jpg“, posted by nDoet: https://mywonderwall.wordpress.com/tag/the-dark-knight/ © Warner Bros. Entertainment Inc.
Vgl. „The Dark Knight“ (dt. „Der Dunkle Ritter“), Christopher Nolan, 2008: https://de.wikipedia.org/wiki/The_Dark_Knight

Folie 8

[Anm.: Bildnachweis:
„the_dark_knight.jpg“: http://reelthinking.wordpress.com/2011/12/27/the-dark-knight/
© Warner Bros. Entertainment Inc.]

Bildnachweis:
„the_dark_knight.jpg“: http://reelthinking.wordpress.com/2011/12/27/the-dark-knight/ © Warner Bros. Entertainment Inc.
Vgl. „The Dark Knight“ (dt. „Der Dunkle Ritter“), Christopher Nolan, 2008: https://de.wikipedia.org/wiki/The_Dark_Knight

Anhang 5
„Vom Sinn der Überwachung“ - Präsentationsfolien der Veranstaltung

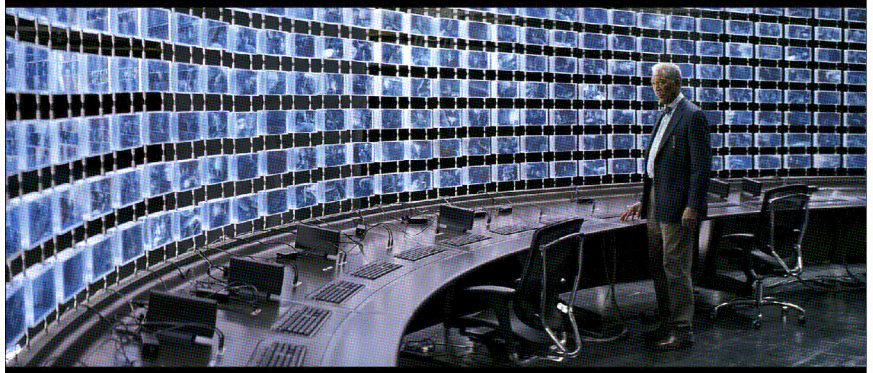
Folie 9

[Anm.: Bildnachweis:
„kinopoisk_ru-dark-knight_2c-the-797889-w-1600.jpg“:
https://pabblogger.wordpress.com/2011/03/02/wallpapers-batman-the-dark-knight/
© Warner Bros. Entertainment Inc.]

Bildnachweis:
„kinopoisk_ru-dark-knight_2c-the-797889-w-1600.jpg“: https://pabblogger.wordpress.com/2011/03/02/wallpapers-batman-the-dark-knight/ © Warner Bros. Entertainment Inc.
Vgl. „The Dark Knight“ (dt. „Der Dunkle Ritter“), Christopher Nolan, 2008: https://de.wikipedia.org/wiki/The_Dark_Knight

Folie 10

Überwachungsszenario...



...in der Vorstellung von Hollywood (2008)

[Anm.: Bildnachweis:
„screenshot-lrg-26.png“: http://media.cinemasquid.com/blu-ray/titles/batman-the-dark-knight/2415/screenshot-lrg-26.png © Warner Bros. Entertainment Inc.]

Bildnachweis:
„screenshot-lrg-26.png“: http://media.cinemasquid.com/blu-ray/titles/batman-the-dark-knight/2415/screenshot-lrg-26.png © Warner Bros. Entertainment Inc.
Vgl. „The Dark Knight“ (dt. „Der Dunkle Ritter“), Christopher Nolan, 2008: https://de.wikipedia.org/wiki/The_Dark_Knight

Folie 11

Retrospektive

„Die Anspielungen auf aktuelle Situationen des "War on Terror" nimmt man besser erst gar nicht ernst.“

(Barbara Schweizerhof, TAZ, 30.07.2008)

[Anm.: Quelle: Barbara Schweizerhof: »"Batman"-Verfilmung "Dark Knight" - Das Sommergespenst«, TAZ, 30.07.2008: http://www.taz.de/!20751/]

Zitat:
Barbara Schweizerhof: "Batman"-Verfilmung "Dark Knight" - Das Sommergespenst, TAZ, 30.07.2008: http://www.taz.de/!20751/

Folie 12

„Die wahren Stars des Abends“

- Doris Aschenbrenner
- PD Dr. Anne Käfer
- Nele Trenner

Anhang 5

„Vom Sinn der Überwachung“ - Präsentationsfolien der Veranstaltung

Folie 13

Vom Sinn der Überwachung

Überwachung und Gesellschaft – eine notwendige Verbindung?

19:15 - 19:25 (10min) Einführung
19:25 - 19:45 (20min) Thesen der Gastrednerinnen
19:45 - 20:25 (40min) Podiumsdiskussion
20:25 - 20:35 (10min) Pause
20:35 - 21:20 (45min) Offene Diskussion
21:20 - 21:30 (10min) Verabschiedung

Moderation:
Alexander Czekalla und Roland Hummel

Bildnachweis:
"Internet Map city-to-city connections" © Chris Harrison:
http://www.chrisharrison.net/index.php/Visualizations/InternetMap
(Modifikation mit Genehmigung des Künstlers)

Folie 14

Pause

10min

Folie 15

Vom Sinn der Überwachung

Überwachung und Gesellschaft – eine notwendige Verbindung?

19:15 - 19:25 (10min) Einführung
19:25 - 19:45 (20min) Thesen der Gastrednerinnen
19:45 - 20:25 (40min) Podiumsdiskussion
20:25 - 20:35 (10min) Pause
20:35 - 21:20 (45min) Offene Diskussion
21:20 - 21:30 (10min) Verabschiedung

Moderation:
Alexander Czekalla und Roland Hummel

Bildnachweis:
"Internet Map city-to-city connections" © Chris Harrison:
http://www.chrisharrison.net/index.php/Visualizations/InternetMap
(Modifikation mit Genehmigung des Künstlers)

Folie 16

Verabschiedung

- www.Jahr1nachSnowden.de
- Bitte um Kritik (und ggf. Empfehlung)
- Einladung zur Praxisveranstaltung
- Abschlussgedanke

Anhang 5
„Vom Sinn der Überwachung“ - Präsentationsfolien der Veranstaltung

Folie 17

„1984“

...in der Rezeption von Apple Inc.

[Anm.: Bildnachweise: https://en.wikipedia.org/wiki/File:Ad_apple_1984.jpg#mediaviewer/File:Ad_apple_1984.jpg https://en.wikipedia.org/wiki/File:Ad_apple_1984_2.png#mediaviewer/File:Ad_apple_1984_2.png]

Folie 18

[Anm.: Videonachweis: Ausschnitt aus „1983 Apple Keynote-The "1984" Ad Introduction“, Youtube-Kanal „The Apple History Channel“: https://www.youtube.com/watch?v=lSiQA6KKyJo]

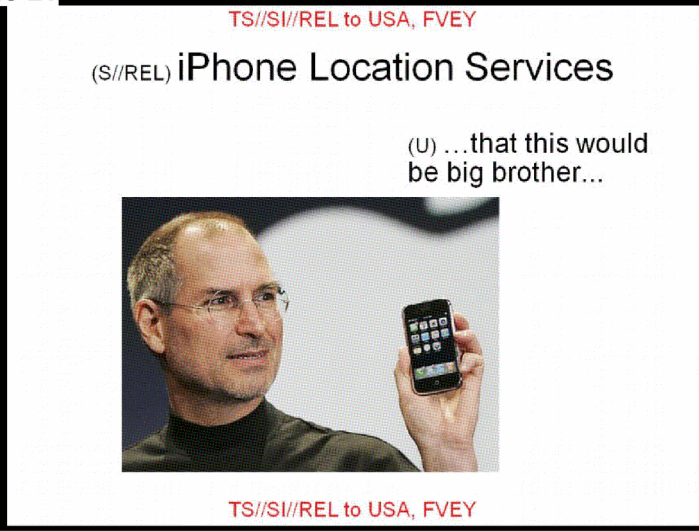
Folie 19

„1984“

...in der Rezeption der NSA

[Anm.: Bildnachweis: „image-541996-galleryV9-uueh.jpg“, Spiegel Online International: „Photo Gallery: Spying on Smartphones“: http://www.spiegel.de/fotostrecke/photo-gallery-spying-on-smartphones-fotostrecke-101201.html]

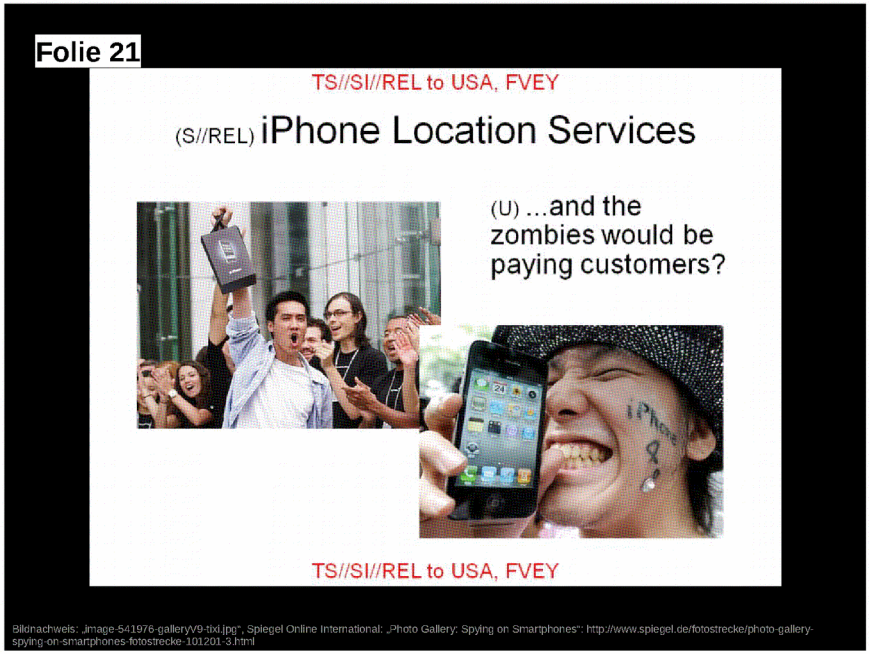
Folie 20



[Anm.: Bildnachweis: „image-541991-galleryV9-gxcl.jpg“, Spiegel Online International: „Photo Gallery: Spying on Smartphones“: http://www.spiegel.de/fotostrecke/photo-gallery-spying-on-smartphones-fotostrecke-101201-2.html]

Anhang 5

„Vom Sinn der Überwachung“ - Präsentationsfolien der Veranstaltung



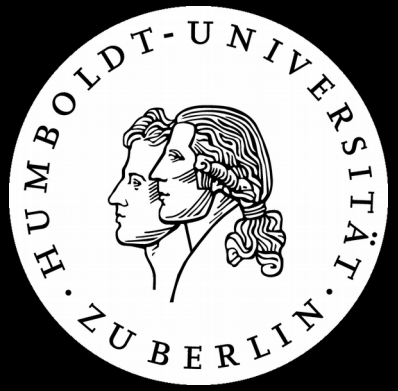
[Anm.: Bildnachweis: „image-541976-galleryV9-tixi.jpg“, Spiegel Online International: „Photo Gallery: Spying on Smartphones“: http://www.spiegel.de/fotostrecke/photo-gallery-spying-on-smartphones-fotostrecke-101201-3.html]

Rollentausch: (sich) selbst überwachen!

www.Jahr1nachSnowden.de

Herzlich willkommen!

(Hinweis: Bitte noch nicht am PC anmelden!)



Tutoren:
Amon Kaufmann
Roland Hummel

Einstieg

1. Wer wir sind
2. Was wir heute (nicht) machen
3. Zeitplan
4. Lageplan
5. Fragen?

Theorieteil 1/4

Soziales Netzwerk analysieren:

Facebook und **NameGenWeb**

Theorieteil 2/4

Emailverkehr analysieren:

GMail

Immersion (MIT)

MUSE (Stanford)

Theorieteil 3/4

Webseitenstruktur „**crawlen**“:

webmasterworld.com

jahr1nachsnowden.de

Theorieteil 4/4

Profilanalyse:

Google-Standardsuche

Freiwillige?

Theorie-Zusatz 1/3

PleaseRobMe.com

Theorie-Zusatz 2/3

Gelocation-„Feature“

Theorie-Zusatz 2/3

Wireshark

Pause

10min

Praxisteil 1/3

Do**I**t**Y**ourself

- einzeln oder in Gruppen

- frei oder nach Aufgaben

Praxisteil 1/3 (Aufgaben)

1. (falls vorhanden:) Analysiere die sozialen Verbindungen deines **Facebook**-Profils!

https://apps.facebook.com/namegenweb/

2. Analysiere die Korrespondenz deines GMail-Accounts mit **Immersion** oder **MUSE**!

https://immersion.media.mit.edu

http://mobisocial.stanford.edu/muse

3. „**Crawle**“, womit sich z. B. folgende Seiten auseinandersetzten, ohne sie direkt zu besuchen:

- roland-schmidt.com
- heldenwelt.de

http://kurzlink.de/MdMY2TipL

4. Schätze die Gefahr von getwitterten Aufenthaltsorten mittels **pleaserobme.com** ein!

http://pleaserobme.com/

5. **Google**, was Amon „letzten Sommer“ getan hat!

http://kurzlink.de/Es3vEs8O5

6. Alles langweilig? Frage nach einem Auftrag für **Wireshark**!

http://test.moodle2.de/

Praxisteil 2/3

Reflexion

Praxisteil 3/3

Empfehlungen:

heise.de/extras/netwars

thenetworkiswatching.com

panopticlick.eff.org

Abschluss

1. nicht zum Angriff, sondern zur **Verteidigung**
2. Bei allen Anwendungen das **Trilemma** durchdenken:
   - komfortabel
   - kostenlos
   - datenschonend
3. **weiterbilden**
4. **relativieren**:

   „Hope the best, expect the worst!“
5. Ausblick: **Komfortzone** verlassen, **digitale Zivilcourage**

Einführung in verschlüsselte Kommunikation

www.Jahr1nachSnowden.de
Herzlich willkommen!

Hinweise:
1. Bitte WLAN einrichten
2. Bitte GnuPG installieren:
https://www.gnupg.org/download/index.html (ganz unten)
3. Name und Emailadresse auf Zettel 1/2 notieren!

Tutor:
Roland Hummel
Initiatoren:
Amon Kaufmann und Roland Hummel

Begrüßung

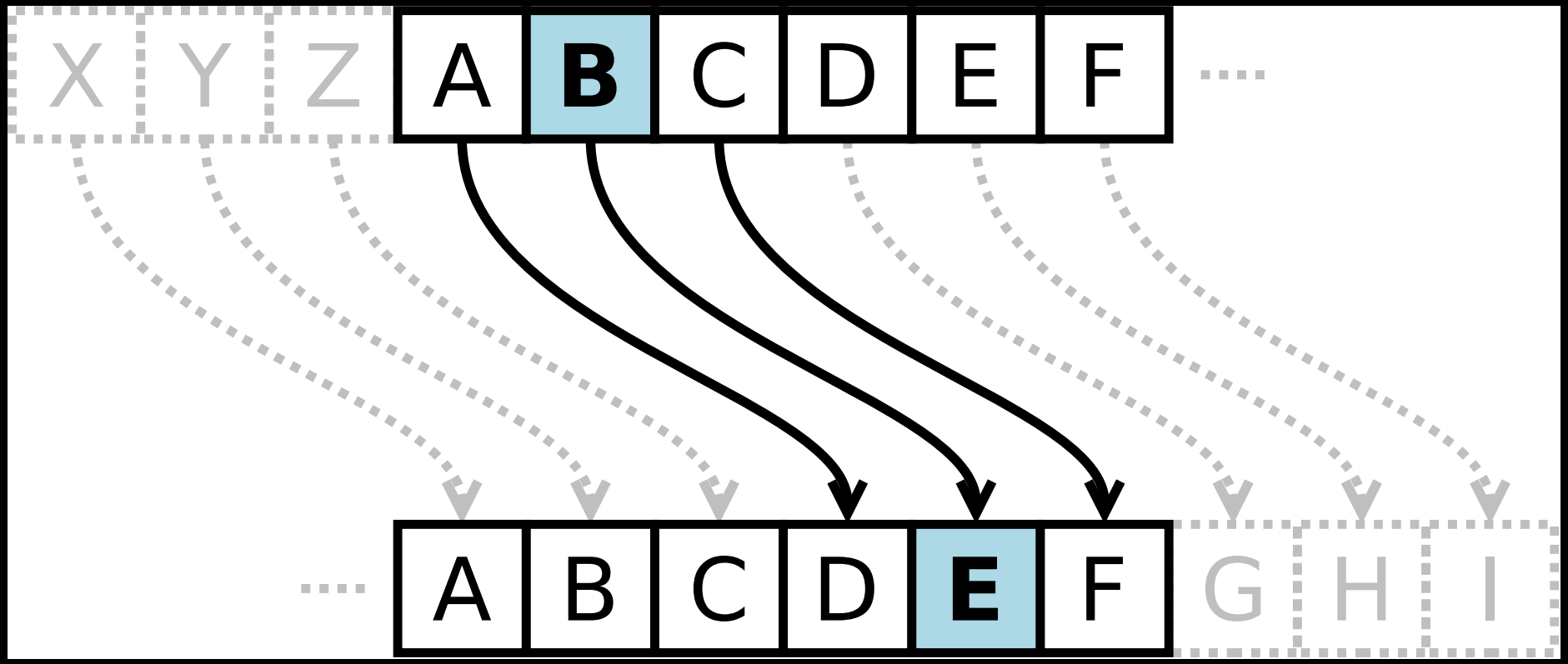
1. Kurzvorstellung
2. Was wir heute (nicht) machen
3. Zeitplan
4. Zettel?
5. Durchhalten!

Teil 1 - Theorie

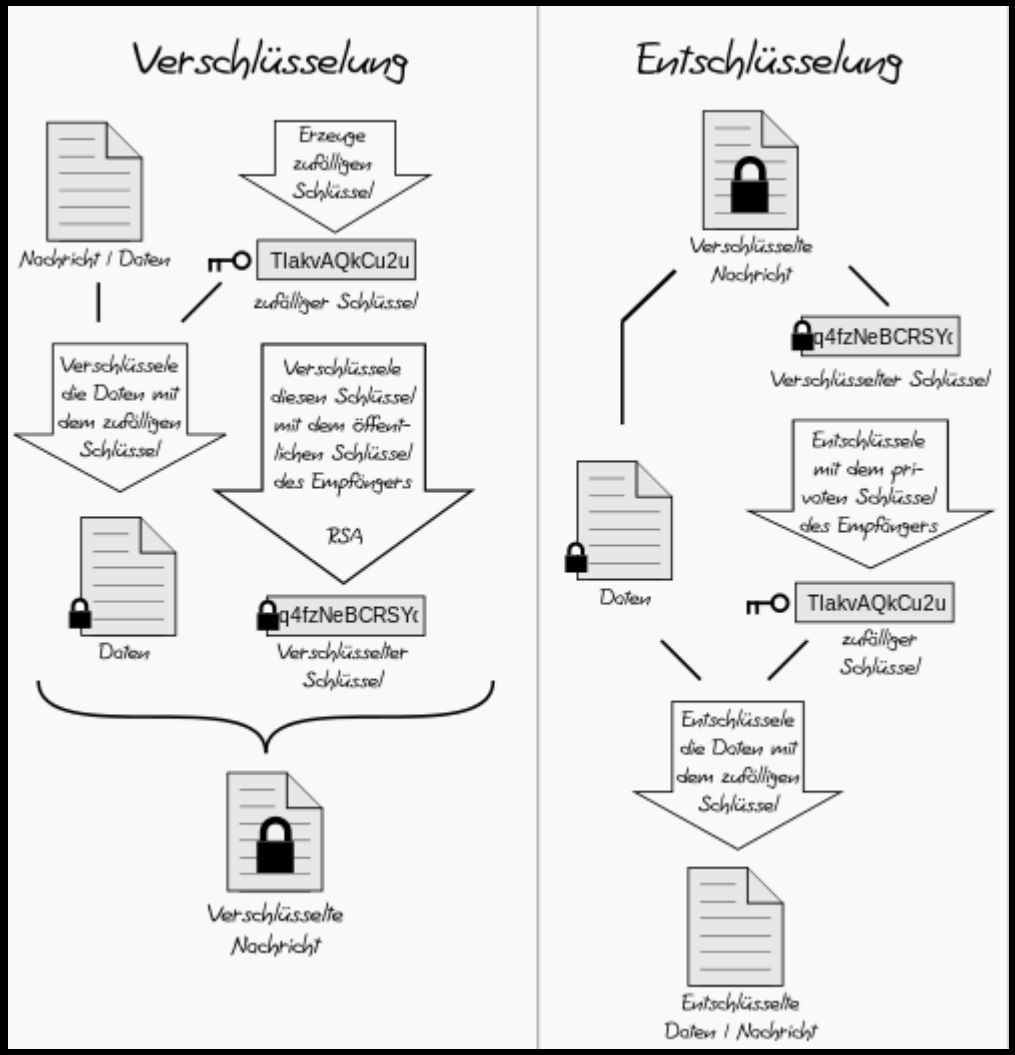
Verschlüsselung

symmetrisch VS **asymmetrische**

Teil 1 – Theorie
symmetrische Verschlüsselung

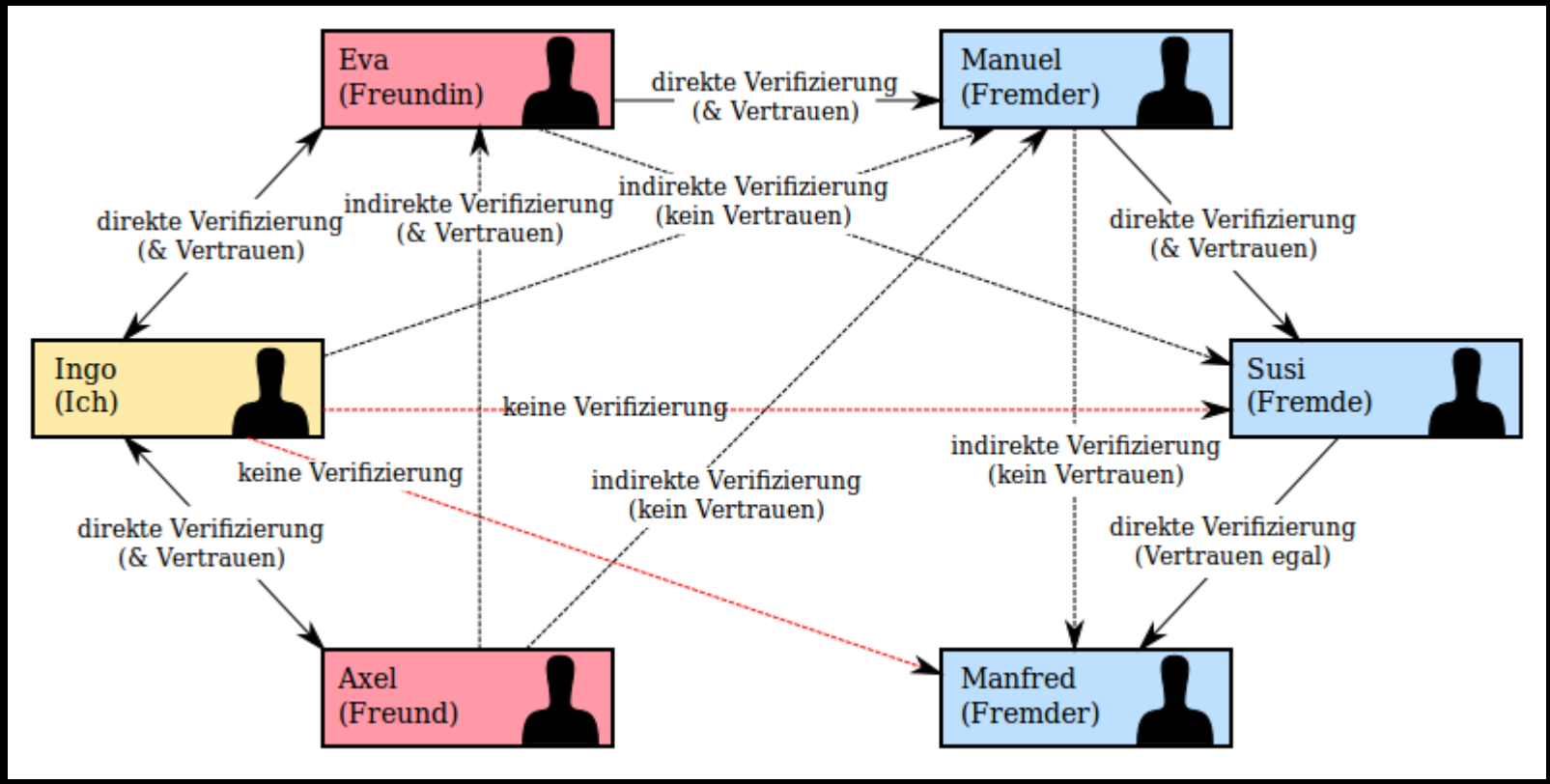


Teil 1 – Theorie
asymmetrische Verschlüsselung



Teil 1 – Theorie

„Web of Trust“



Teil 1 - Theorie

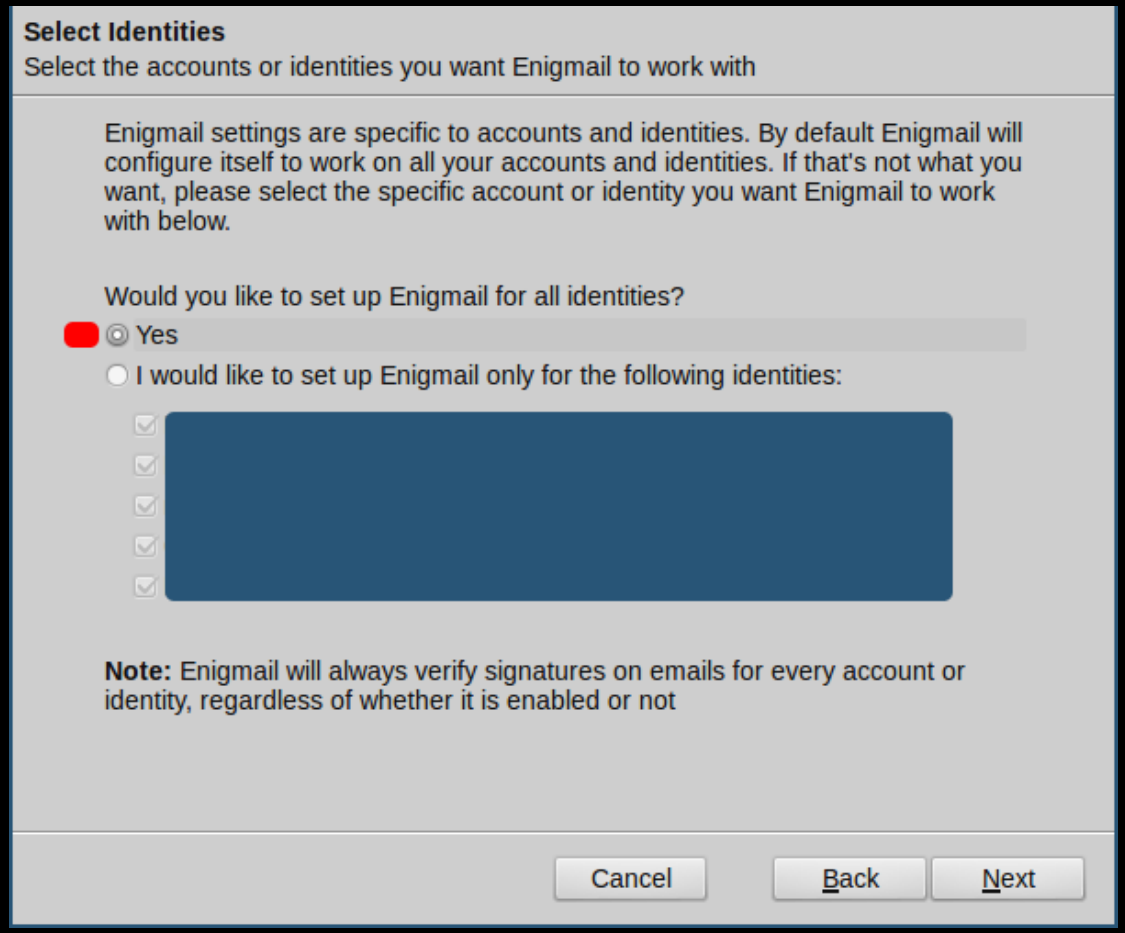
Am Beispiel

Thunderbird und **Enigmail**

Teil 1 - Theorie

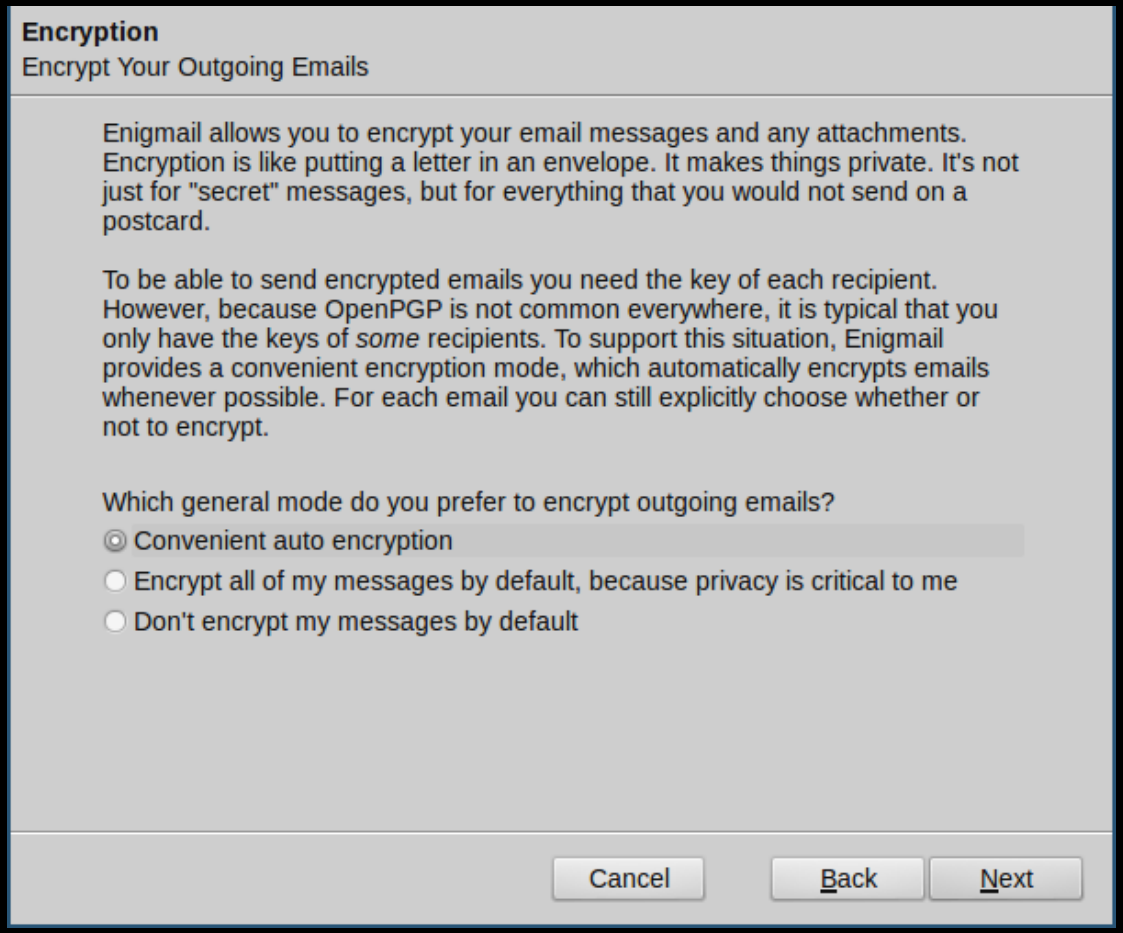
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



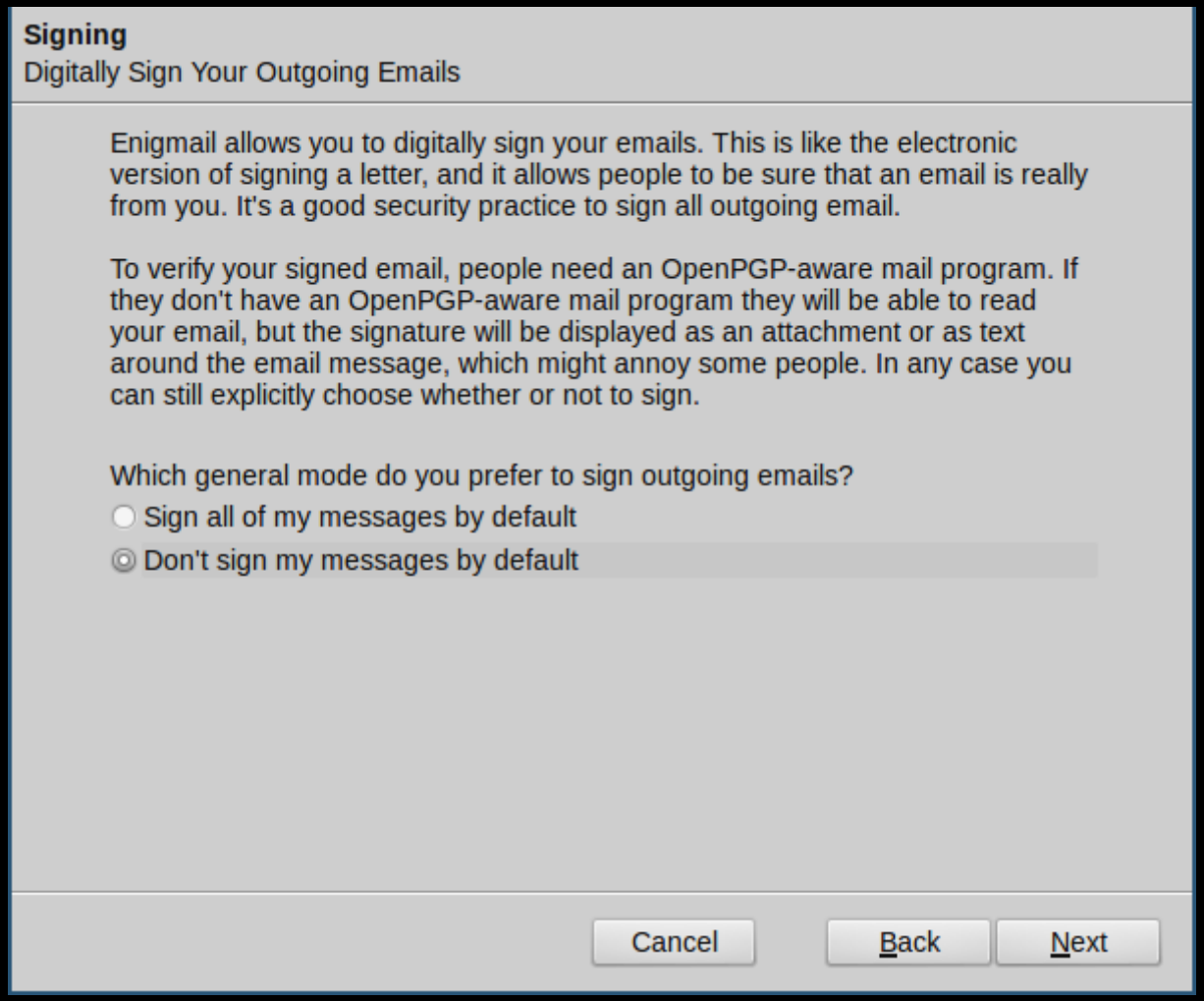
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



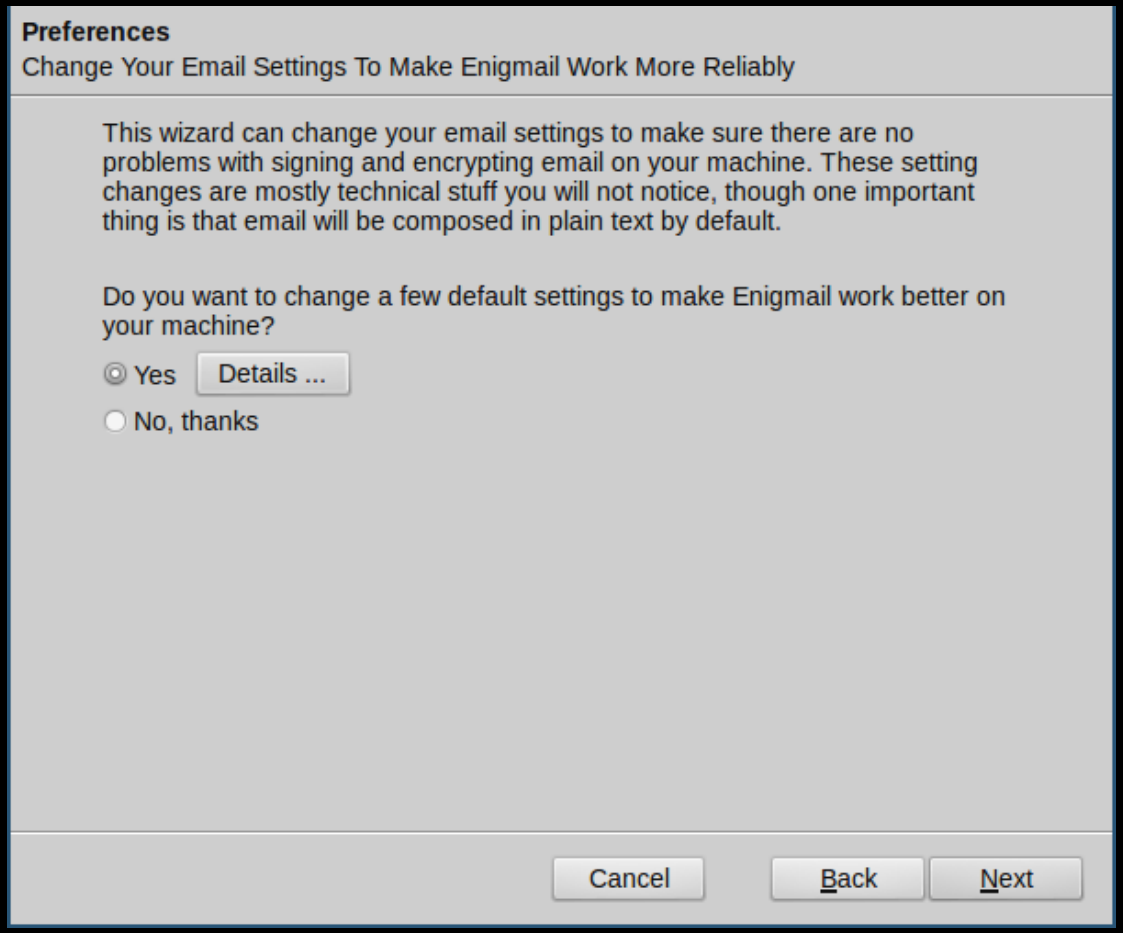
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



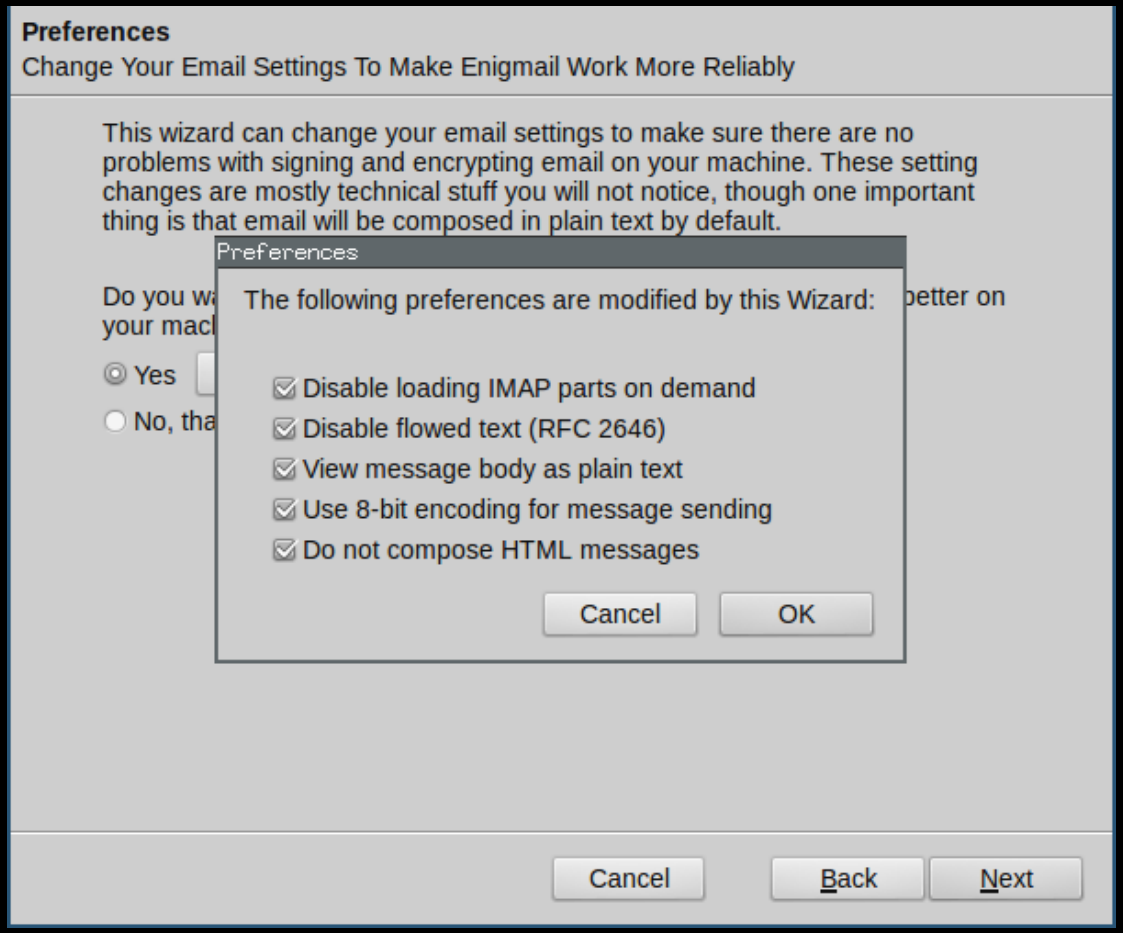
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



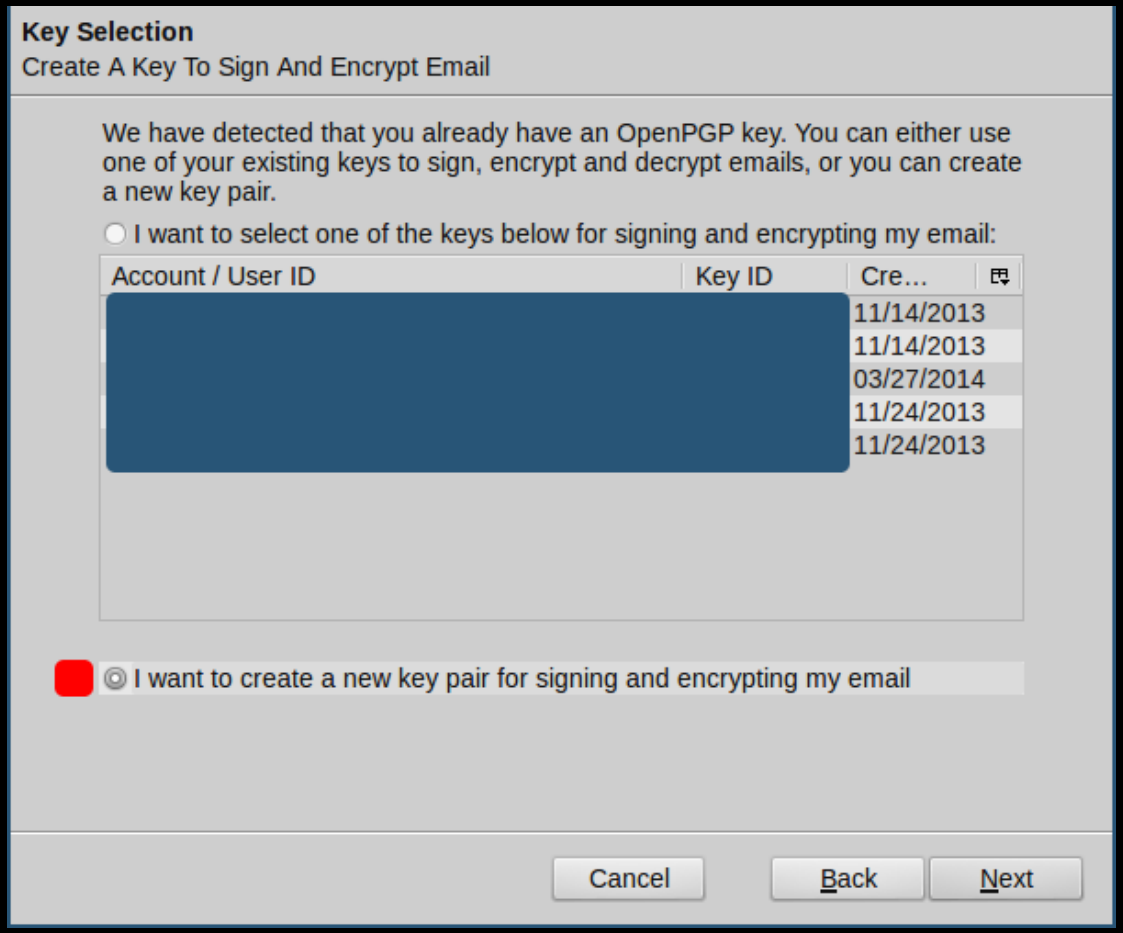
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



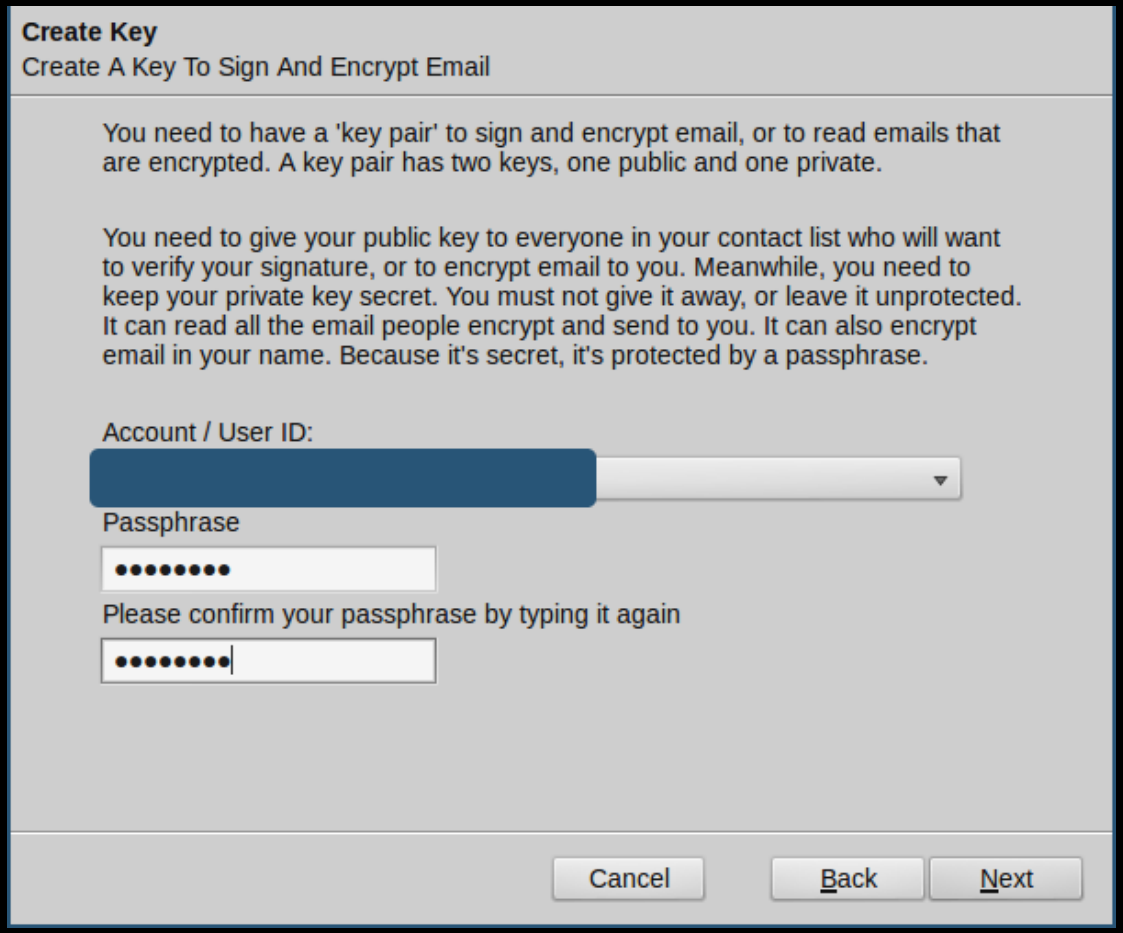
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



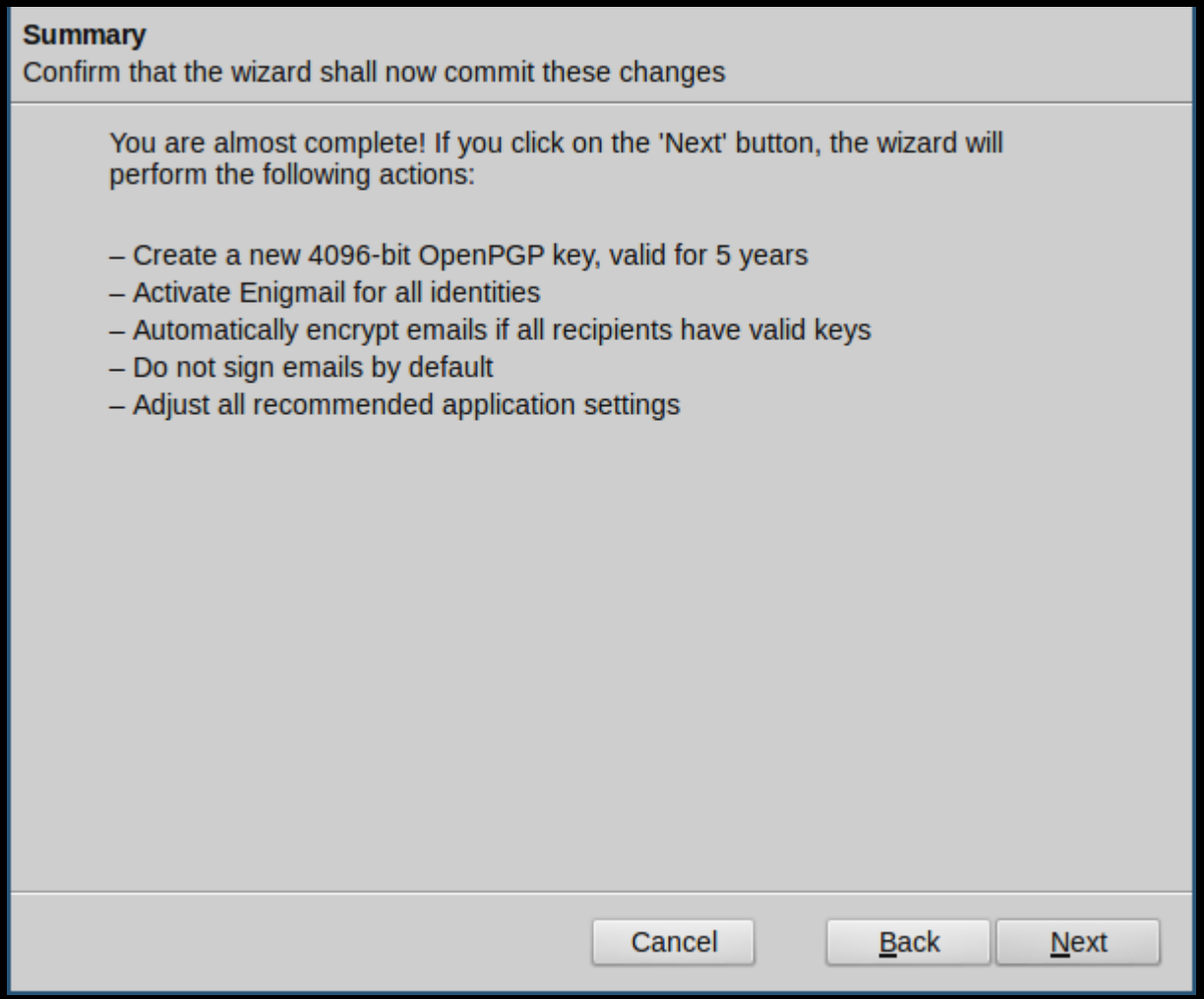
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



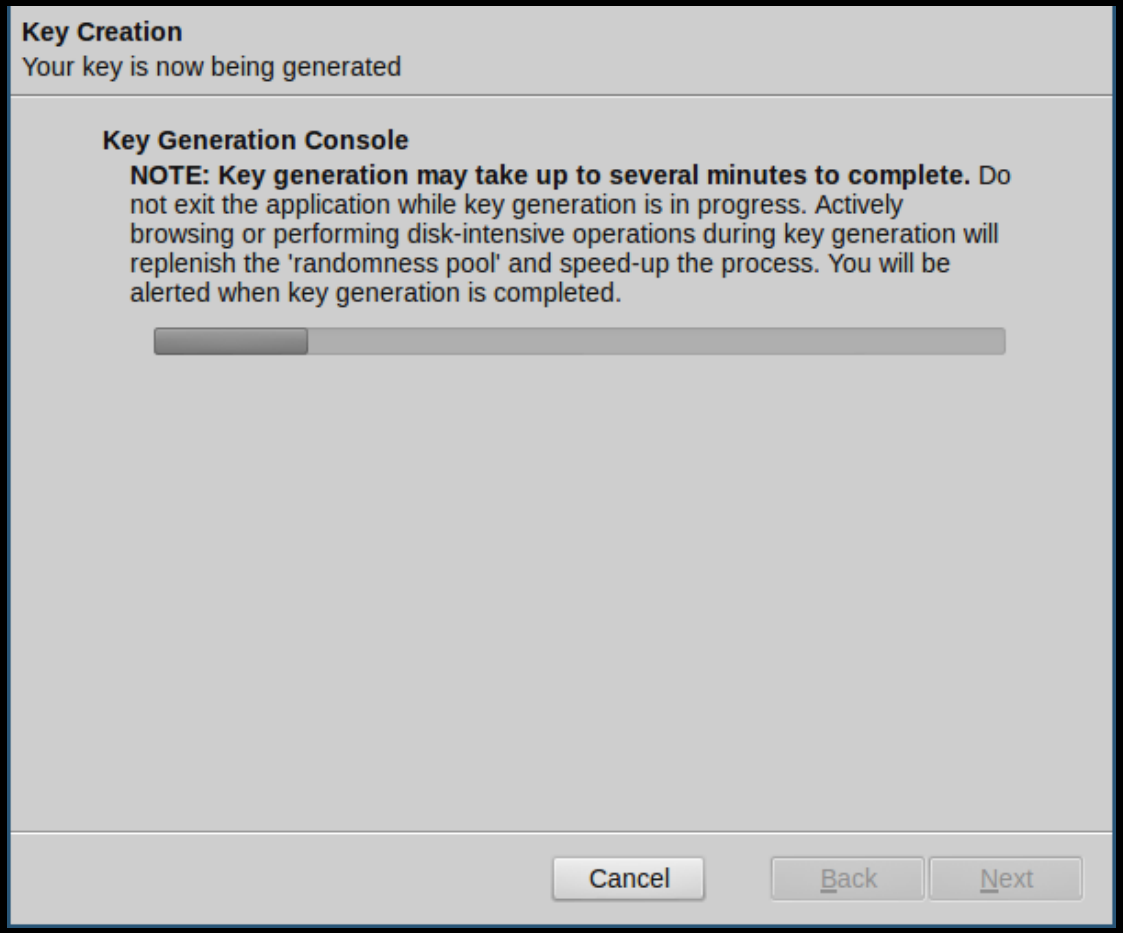
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



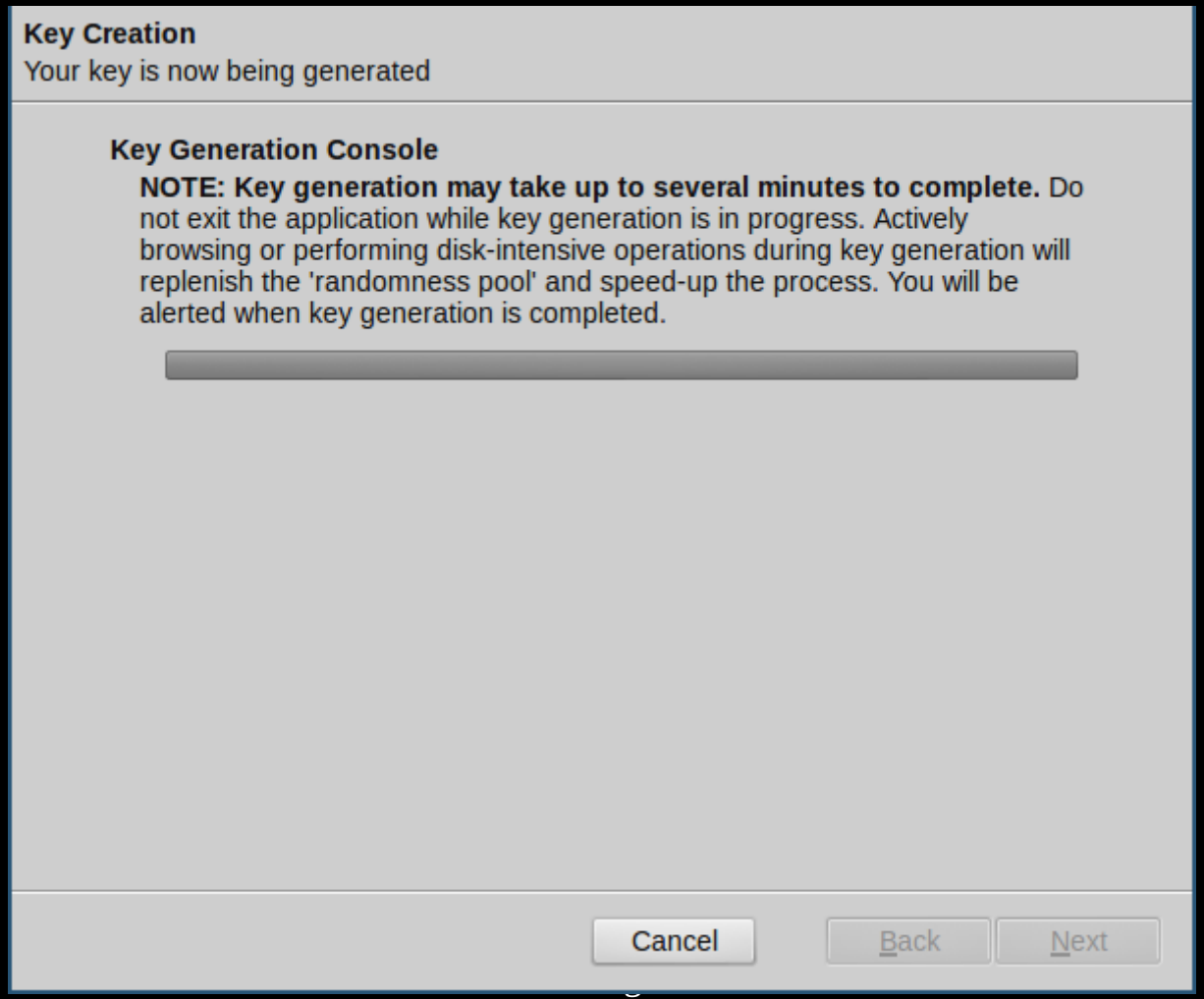
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



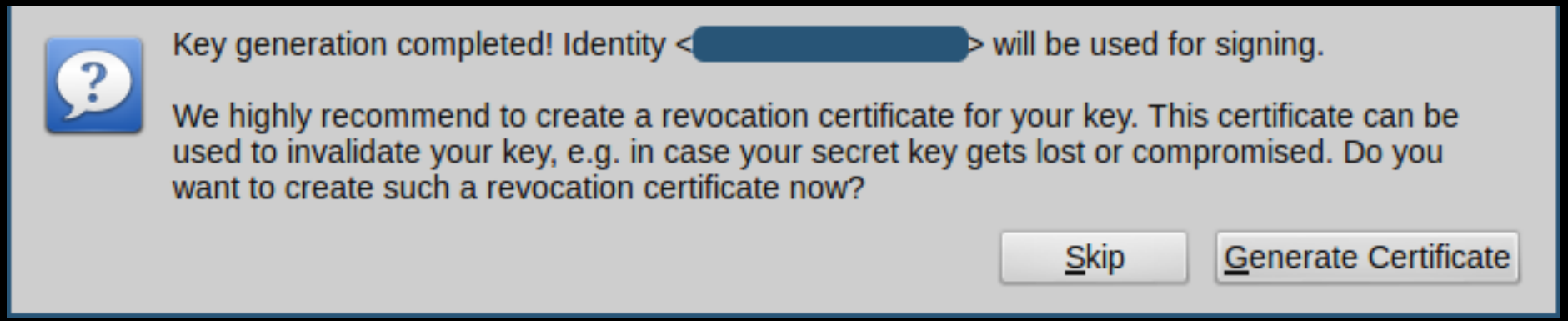
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



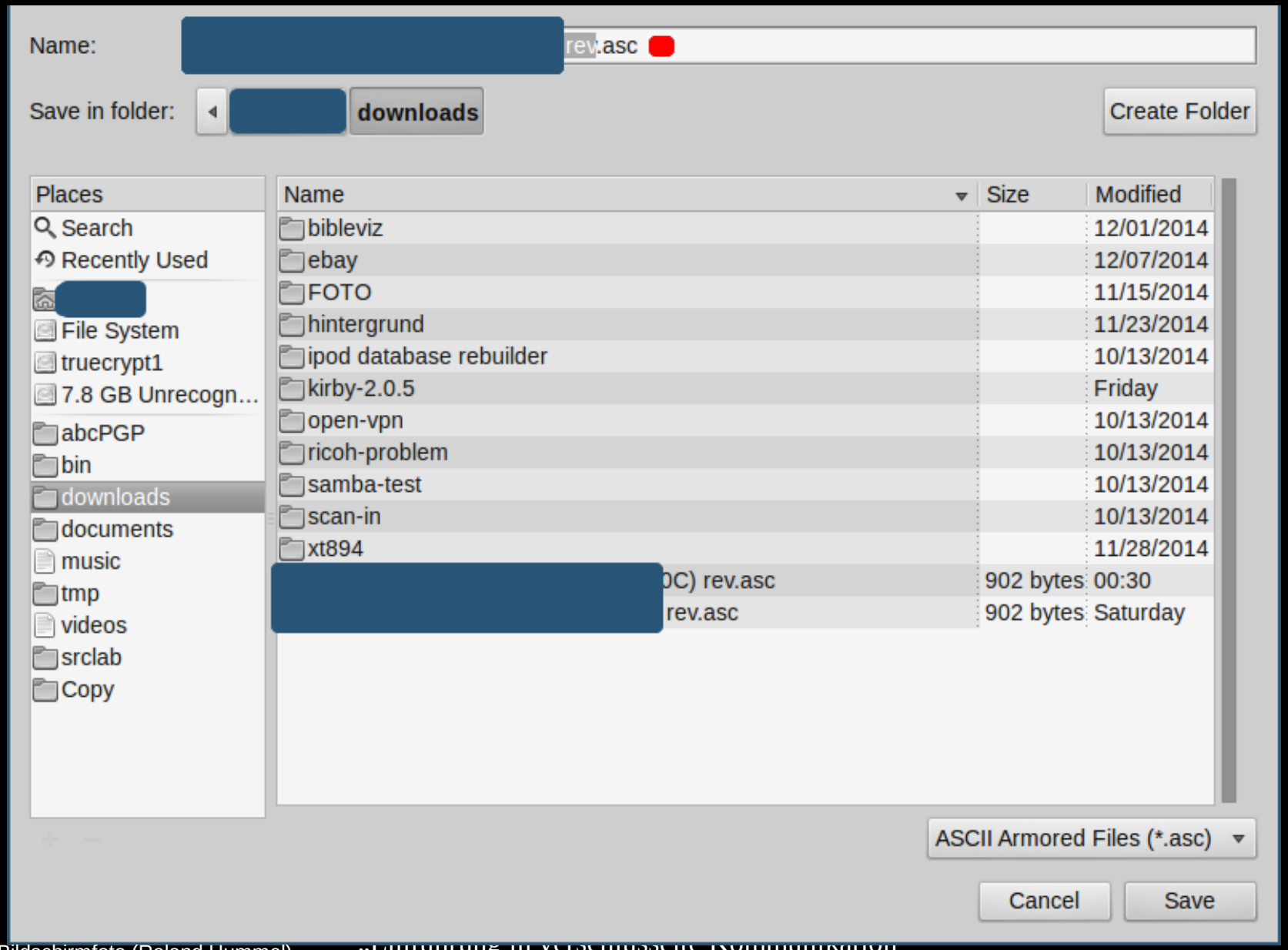
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



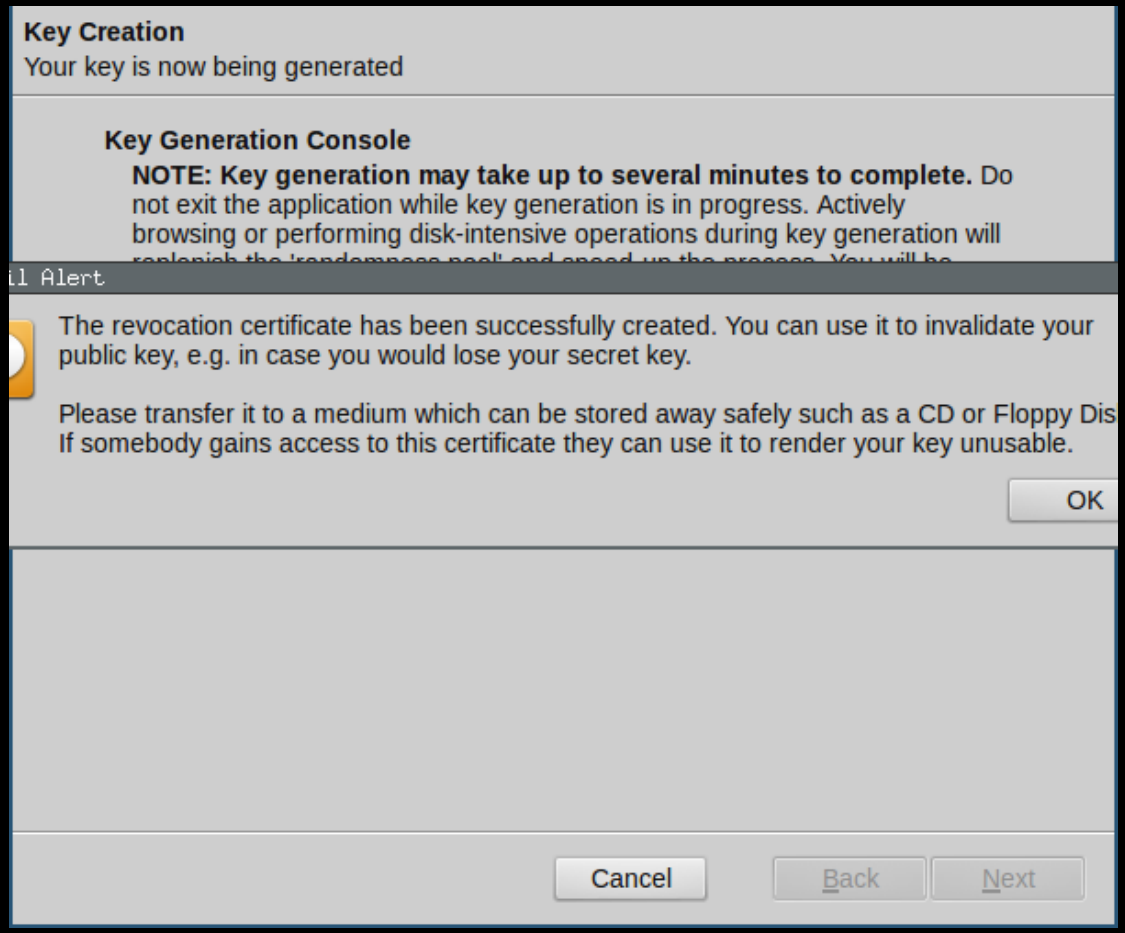
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



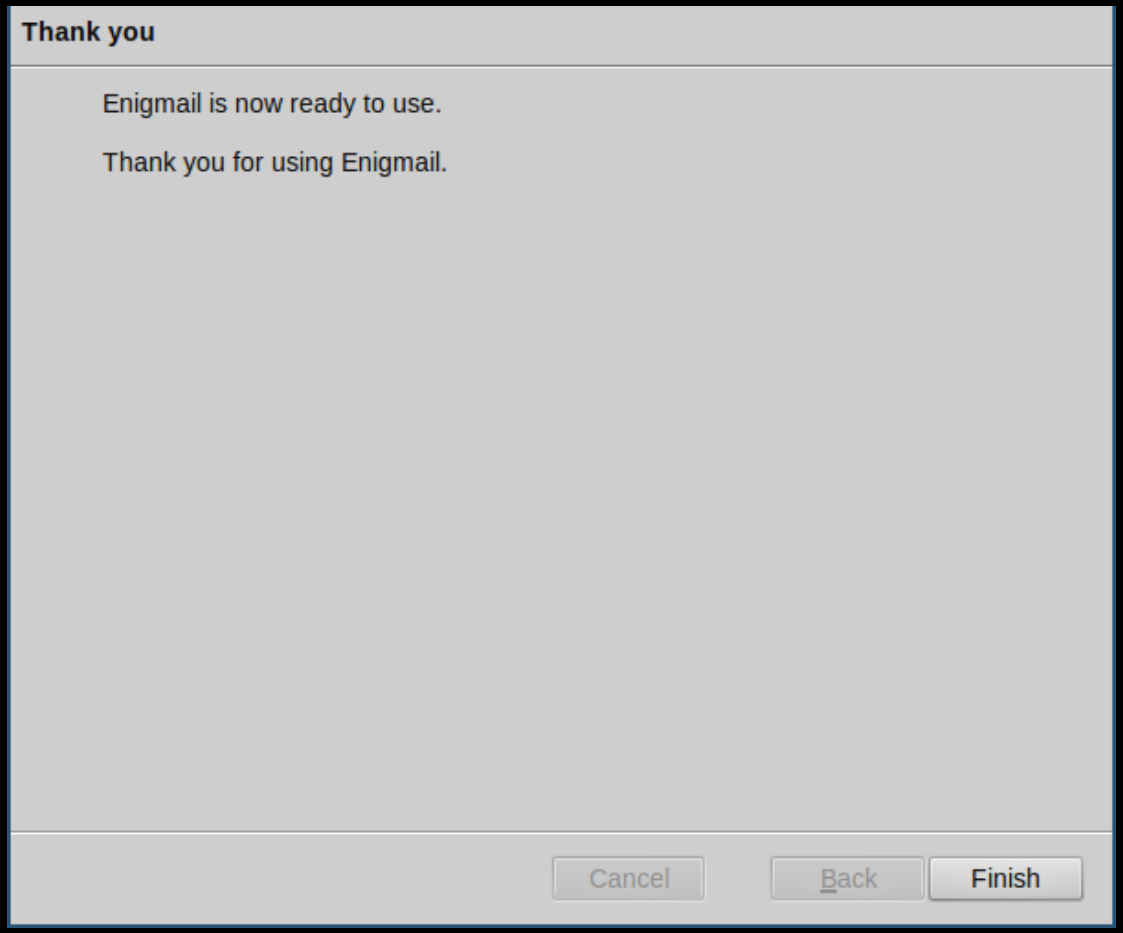
Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie



Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 1 - Theorie

1. öffentlichen Schlüssel **veröffentlichen** (Keyserver und/oder Email)
2. Schlüsselpaar **sichern** / drucken
3. **Widerrufsfunktion**

Pause

10min

Teil 2 - Umsetzung

1.0 GnuPG und Enigmail installieren

-> ggf. Thunderbird neu starten lassen und autom. Wizard folgen:

1.1 „für alle Identitäten?“ - ja

1.2 „immer verschlüsseln?“ - sofern Key schon vorhanden, ja (1. Option)

1.3 „immer signieren?“ - nein (erstmal nicht)

1.4 „Eintellungen angleichen“? - ja

1.5 „Neues Schlüsselpaar erstellen?“ - ja

1.6 Account/ID auswählen – Passwort wählen (kann nachträglich geändert werden)
Hinweis: sichere(re)s Passwort mit http://kurzlink.de/vuaf2BL6M erstellen

-› Email-Adresse, Key-ID und PW auf *privatem* Zettel notieren und *privat* halten!

1.7 Zusammenfassung bestätigen

1.8 Schlüsselerzeugung abwarten

1.9 „Widerrufszertifikat erstellen?“ - ja (Passwort bei Abfrage *nie* speichern, Warnung bestätigen, fertig)

1.10 öffentlichen Schlüssel veröffentlichen (Keyserver und/oder Email)

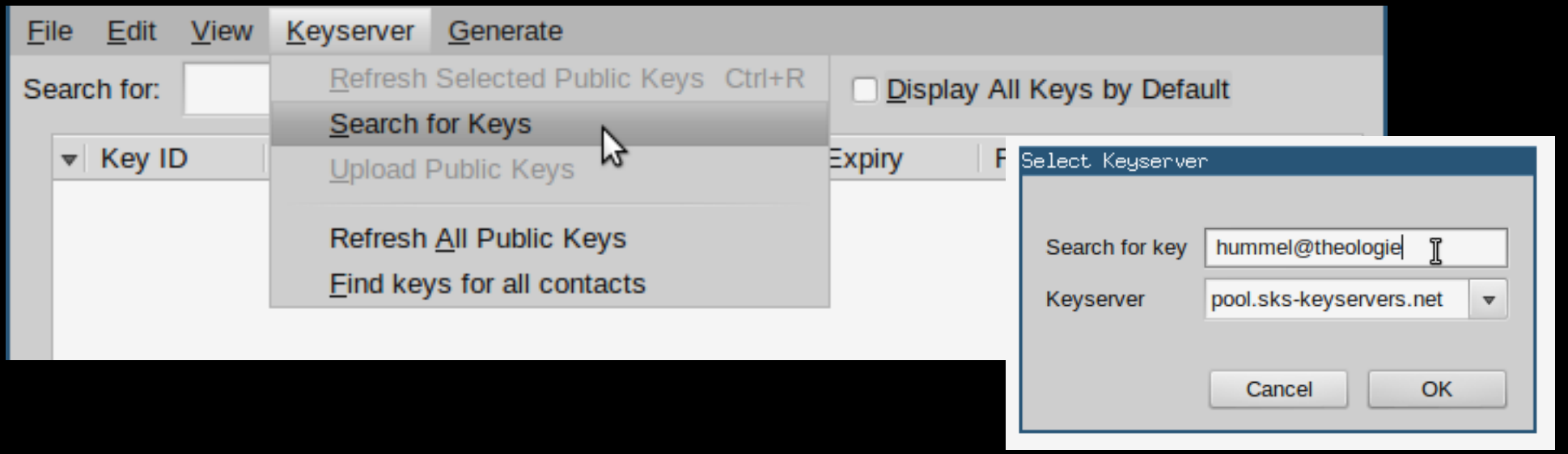
1.11 Schlüsselpaar sichern / drucken

1.12 Widerrufsfunktion zeigen

Teil 2 - Umsetzung

2. Erster Mailwechsel: Email an Sitznachbar (→ Zettel Uhrzeigersinn)

2.1.1 entweder sofort verschlüsselt mit Keyserver-Suche über Enigmail/Schlüsselverwaltung oder online (Keyserver: http://kurzlink.de/vuaf2BL6M → Synchronisation dauert etwas)



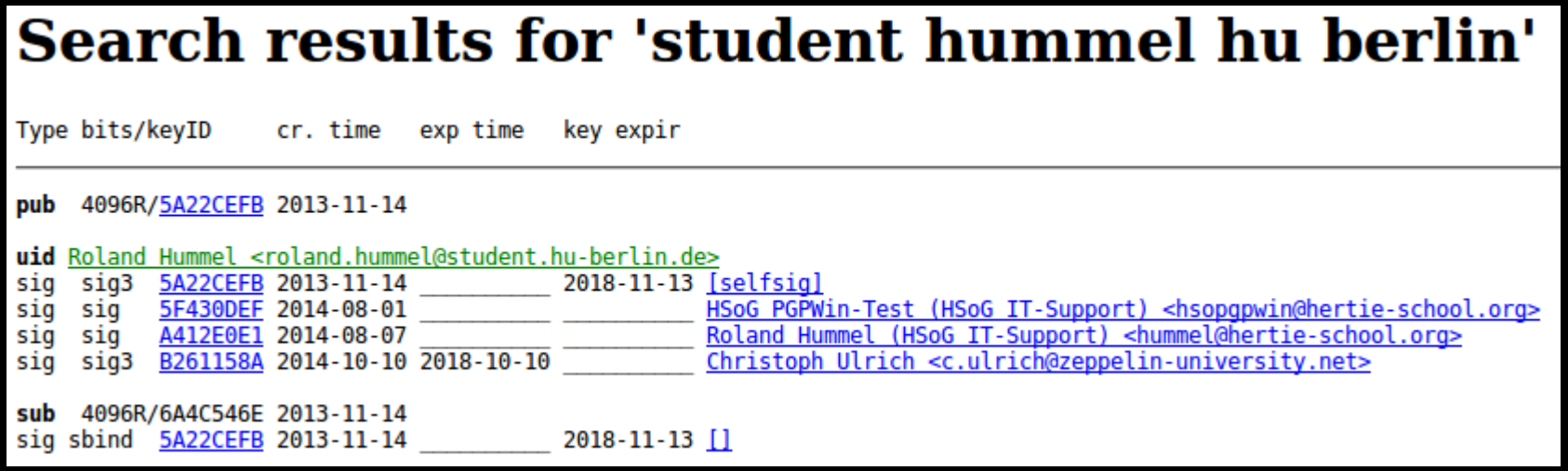
2.1.2 ohne Wartezeit auf den Keyserver ersteinmal *unverschlüsselt* (nur Signierung ist schon möglich) für Zusendung des öffentlichen Schlüssels

2.2 empfangenen Schlüssel über Schlüsselverwaltung importieren

2.3 Email verschlüsselt beantworten

Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 2 – Umsetzung
Theorieexkurs 1/3: „Sign Key“-Stufen (sig(0) - sig3)



Search results for 'student hummel hu berlin'

```
Type bits/keyID     cr. time   exp time   key expir
------------------------------------------------------------------------------
pub  4096R/5A22CEFB 2013-11-14

uid Roland Hummel <roland.hummel@student.hu-berlin.de>
sig  sig3  5A22CEFB 2013-11-14 __________ 2018-11-13 [selfsig]
sig  sig   5F430DEF 2014-08-01 __________ __________ HSoG PGPWin-Test (HSoG IT-Support) <hsopgpwin@hertie-school.org>
sig  sig   A412E0E1 2014-08-07 __________ __________ Roland Hummel (HSoG IT-Support) <hummel@hertie-school.org>
sig  sig3  B261158A 2014-10-10 2018-10-10 __________ Christoph Ulrich <c.ulrich@zeppelin-university.net>

sub  4096R/6A4C546E 2013-11-14
sig sbind  5A22CEFB 2013-11-14 __________ 2018-11-13 []
```

Optionen „**Sign Key**“/“Schlüssel unterschreiben“:
1. „I will not answer“/„Keine Antwort“ (=**sig0**)
2. „I have not checked at all“/„Ich habe es nicht überprüft“ (=**sig1**)
3. „I have done casual checking“/„Ich habe es nur einfach überprüft“ (=**sig2**)
4. „I have done very careful checking“/„Ich habe es sehr genau überprüft“ (=**sig3**)

-› öffentliche Info für Schlüsselserver!

[5. Option „Local signature (cannot be exported)“/“Lokal unterschreiben (nicht exportierbar) → Unterschrift bleibt lokal und kann nicht hochgeladen werden]

Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 2 – Umsetzung
Theorieexkurs 2/4: Bedeutung der sig-Stufen

--default-cert-level n
The default to use for the check level when signing a key.

0 means you make no particular claim as to how carefully you verified the key.

1 means you believe the key is owned by the person who claims to own it but you could not, or did not verify the key at all. This is useful for a "persona" verification, where you sign the key of a pseudonymous user.

2 means you did casual verification of the key. For example, this could mean that you verified that the key fingerprint and checked the user ID on the key against a photo ID.

3 means you did extensive verification of the key. For example, this could mean that you verified the key fingerprint with the owner of the key in person, and that you checked, by means of a hard to forge document with a photo ID (such as a passport) that the name of the key owner matches the name in the user ID on the key, and finally that you verified (by exchange of email) that the email address on the key belongs to the key owner.

Note that the examples given above for levels 2 and 3 are just that: examples. In the end, it is up to you to decide just what "casual" and "extensive" mean to you.

This option defaults to 0 (no particular claim).

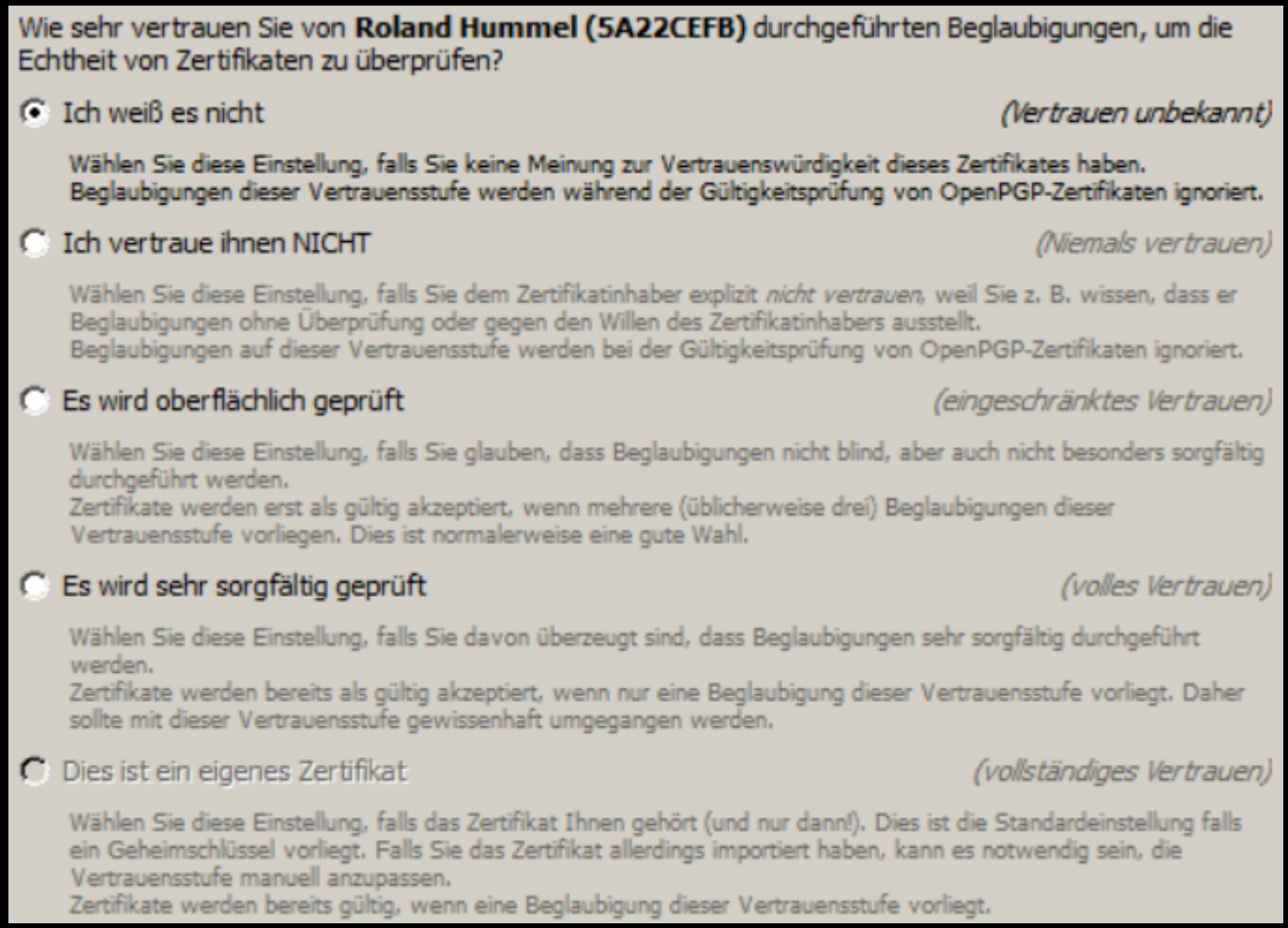
--min-cert-level
When building the trust database, treat any signatures with a certification level below this as invalid. Defaults to 2, which disregards level 1 signatures. Note that level 0 "no particular claim" signatures are always accepted.

Quelle: Manual „gpg - OpenPGP encryption and signing tool", gpg (GNuPG) 1.4.12, Abschnitt „ default-cert-level n"

Teil 2 – Umsetzung
Theorieexkurs 3/4: „Owner Trust“-Optionen (engl.)

Optionen „Set **Owner Trust**“/“Besitzer-Vertrauen festlegen“
1. „I don't know“/„unbekannt“ (Standard)
2. „I do NOT trust“/„kein Vertrauen“
3. „I trust marginally“/„geringes Vertauen“
4. „I trust fully“/„volles Vertrauen“
5. „I trust ultimately“/„absolutes Vertrauen“

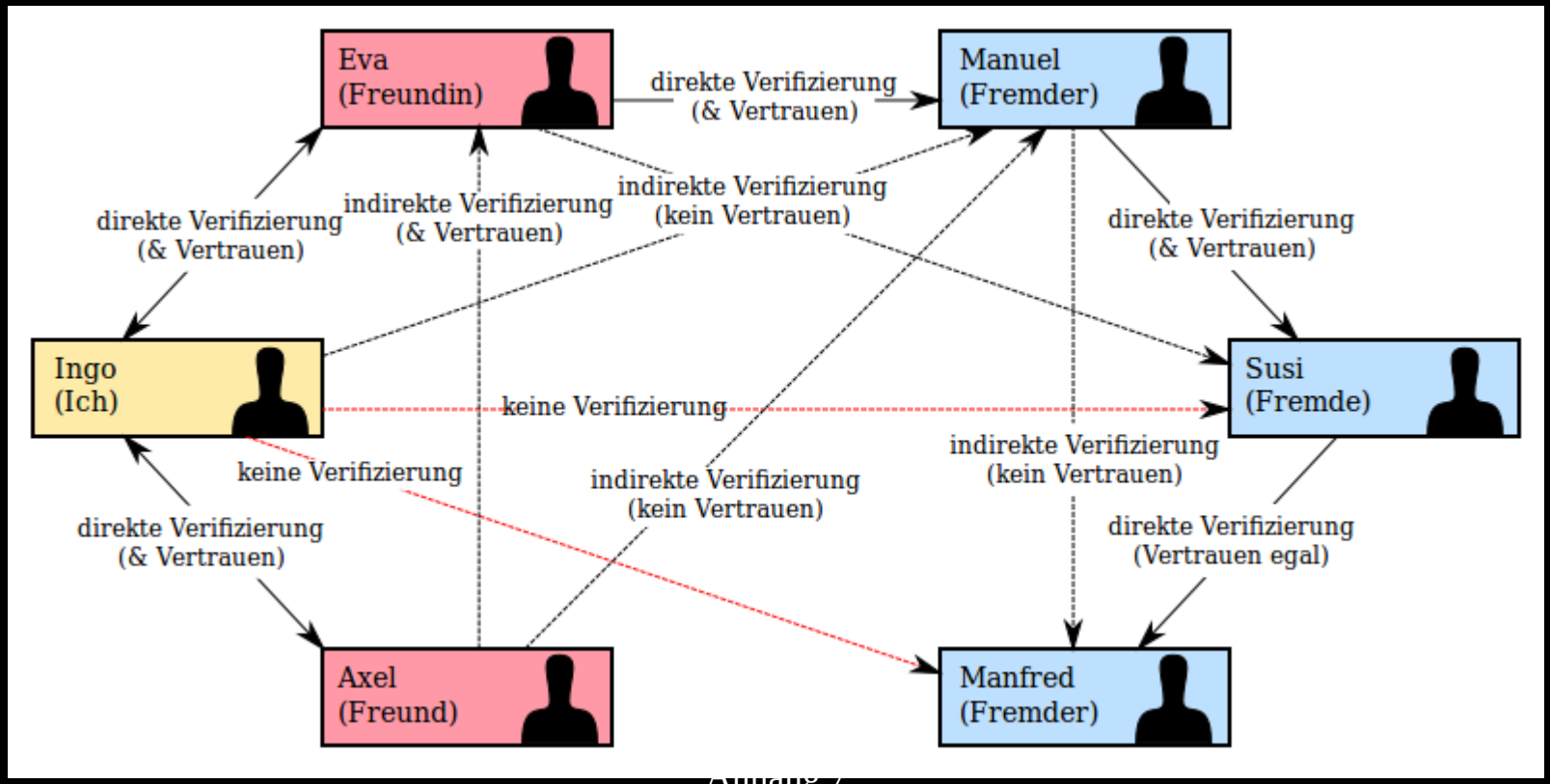
Teil 2 – Umsetzung
Theorieexkurs 3/4: „Owner Trust“-Optionen (dt.)



Bildnachweis: Bildschirmfoto (Roland Hummel).

Teil 2 – Umsetzung
Theorieexkurs 4/4: „Owner Trust“-Auswirkungen

→ (immer individuelle) Vertrauenskategorie
1. bezieht sich immer nur auf die Schlüssel**ersteller,**
2. wird **nie veröffentlicht**
3. kann jederzeit angepasst werden
4. beeinflusst so das *immer persönliche* WoT unmittelbar:



Teil 2 - Umsetzung

3. **Signatur-Warnung** beachten und entsprechend Zertifizierung mit Sitznachbar mittels **Fingerprint** auf öffentlichem **Zettel**

3.1 Zettel mit Fingerprints vergleichen Schlüsselverwaltung+öffentlicher Zettel oder Schlüsselverwaltung+Schlüsselserver

3.2 digital unterschreiben/signieren

3.3 **Owner Trust**/Besitzer-Vertrauen festlegen

Teil 2 - Umsetzung

Zu 3.3) „Set **Owner Trust**“/“Besitzer-Vertrauen festlegen“

1. „I don't know“/„unbekannt“ (Standard)

2. „I do NOT trust“/„kein Vertrauen“

3. „I trust marginally“/„geringes Vertauen“

4. „I trust fully“/„volles Vertrauen“

5. „I trust ultimately“/„absolutes Vertrauen“

→ Vertrauenskategorien bez. sich auf Schlüssel**ersteller (**nie auf einen Schlüssel) und sind **niemals öffentlich!**

Teil 2 - Umsetzung

4. Email beantworten

und

positive Signatur-Meldung

beachten

Teil 3 - Refexion

1. Fragen?

2. drei wichtige Aspekte für erfolgreiche Verschlüsselung:

I – sichere **Technik**

II – sicherer **Umgang**

III – **Konsequenz** in der Anwendung

3. Belohnung: **Unabhängiges, selbstverwaltetes Verfahren** und **„Sand im Getriebe“** der Massenüberwachung

4. verschlüsselter Email**versand** für Leute, die kein PGP nutzen:

https://encrypt.to/

Teil 4 - Übung

2 Möglichkeiten:

1. *öffentlichen* Zettel nochmals mit anderem Partner tauschen und Schritte wiederholen

2. Verständnistest ablegen:

http://openpgp-schulungen.de/verstaendnistest/

Abschluss

1. nur eine **Möglichkeit** unter vielen
2. **Trilemma**:

komfortabel - kostenlos - sicher

3. drei wichtige Aspekte für Verschlüsselung:

I – sichere **Technik -** II – sicherer **Umgang -** III – **Konsequenz** in der Verwendung

4. **Absicherung** der Rechner
5. **Komfortzone, Zivilcourage**
7. **Hilfen**:

amor.cms.hu-berlin.de/~paetzela/

german-privacy-fund.de/e-mails-verschlusseln-leicht-gemacht

Datenhoheit und Datenkontrolle (auch ohne Verschlüsselung)

www.Jahr1nachSnowden.de

Herzlich willkommen!

(Hinweis: Bitte noch nicht am PC anmelden!)

Tutor:
Roland Hummel
Initiatoren:
Amon Kaufmann und Roland Hummel

Einstieg

1. Initiative und Tutor
2. Türproblematik
3. Zeitplan
4. Was wir heute machen
   → erst Theorie, dann Praxis
5. Einführung in Linux inklusive
6. Themenspektrum

Themenspektrum

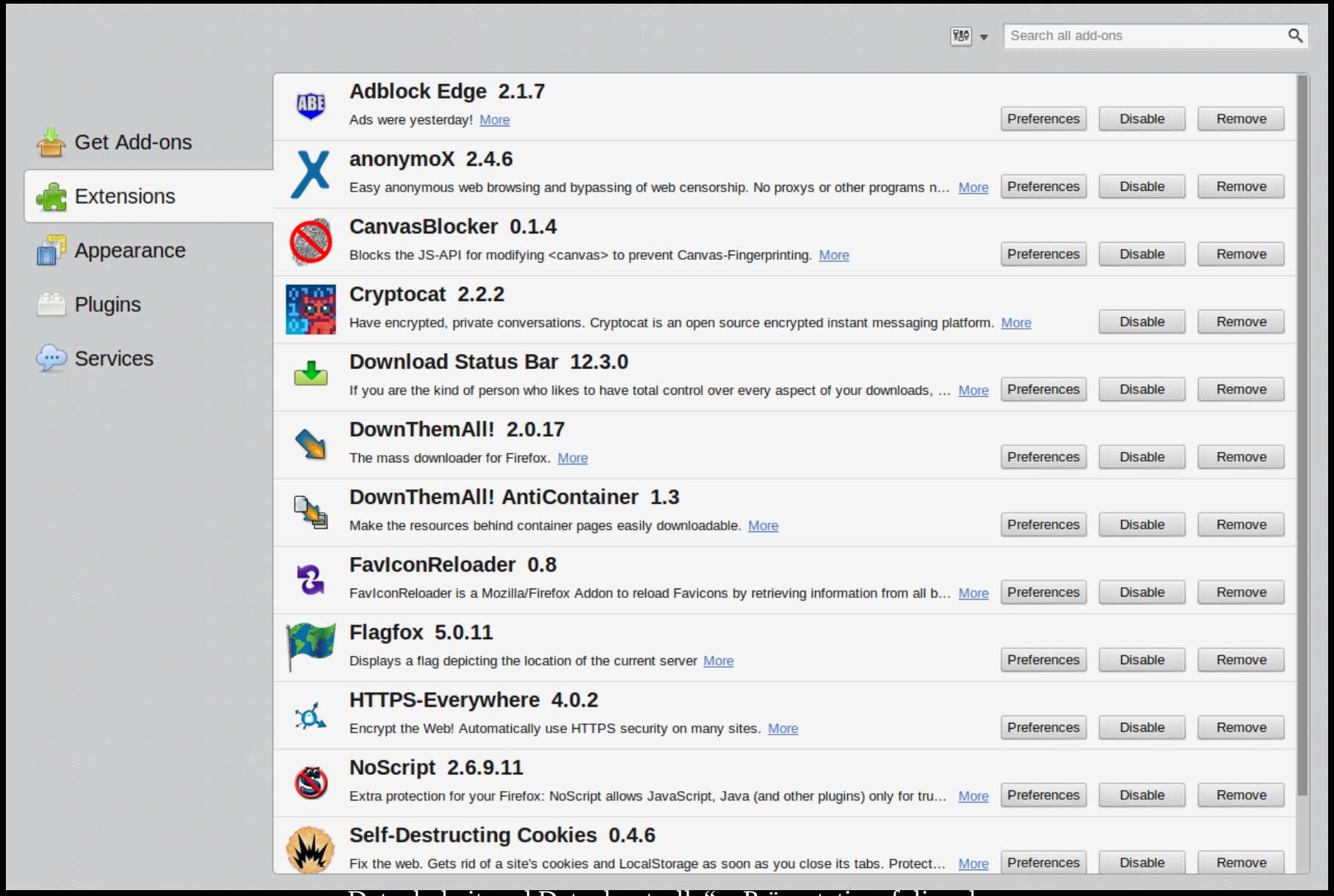
1. sichere(re) Passwörter
2. sichere(re)s Surfen mit Firefox – Add-ons
3. Suchen/Suchmaschinen in Eigenkontrolle (YaCy)
4. Exkursion ins „Invisible Net“ (TOR)

Theorieteil 1/4 - sichere(re) Passwörter

3 Konzepte

1. ein „sehr starkes“ PW
2. Master-Passwort: „viele PW durch ein PW“
3. Passwortcontainer

Theorieteil 2/4 - sichere(re)s Surfen



Bildnachweis: Bildschirmfoto (Roland Hummel).

Theorieteil 2/4 - sichere(re)s Surfen

Auswahl aus den Add-ons des Tutors:

1. Adblock Edge
2. anonymoX
3. CanvasBlocker
4. Flagfox
5. HTTPS-Everywhere
6. **NoScript**
7. Self-Destructing Cookies
8. **WOT**

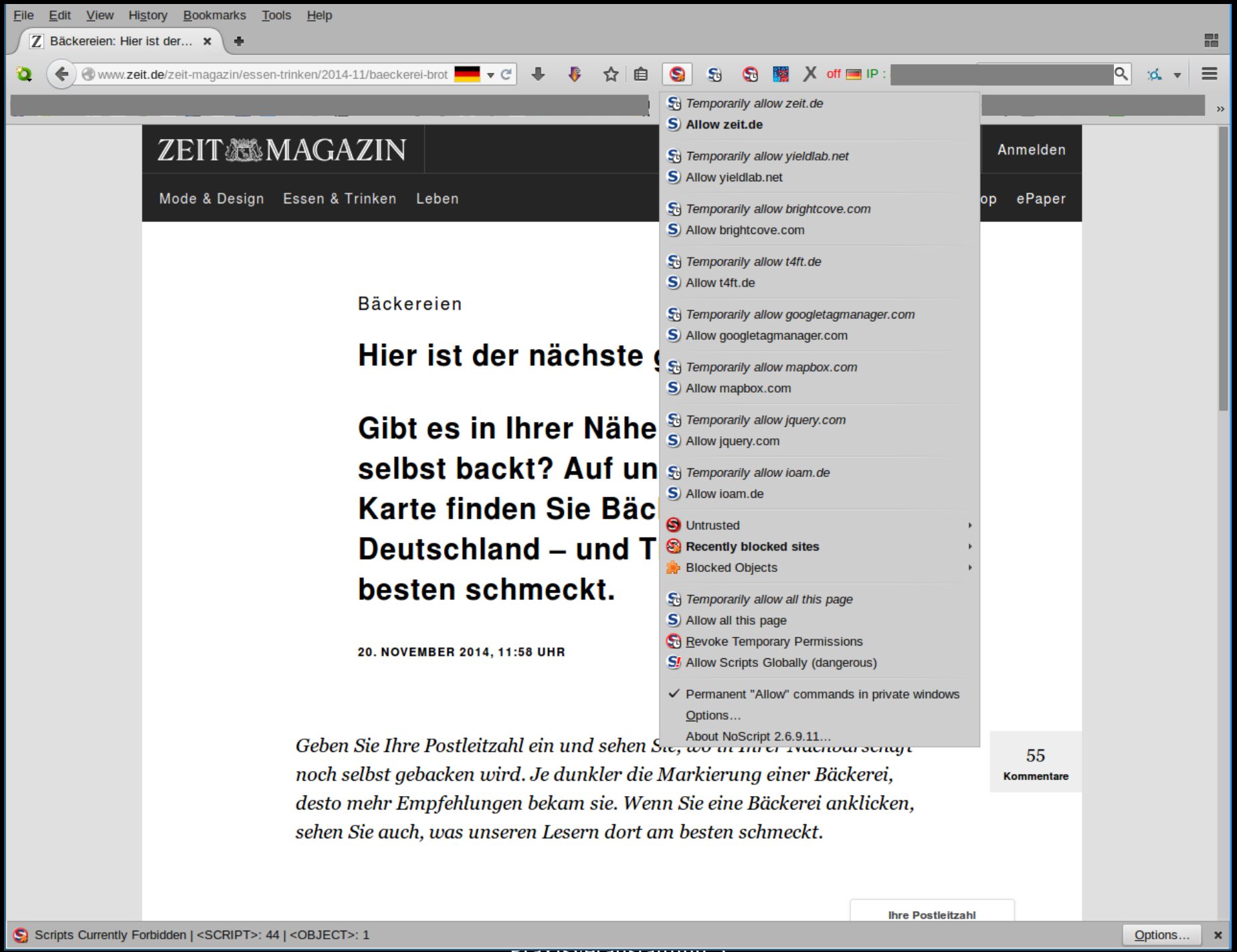
Theorieteil 2/4 - NoScript

1. Installation
2. Anwendung:

→ wikipedia.de

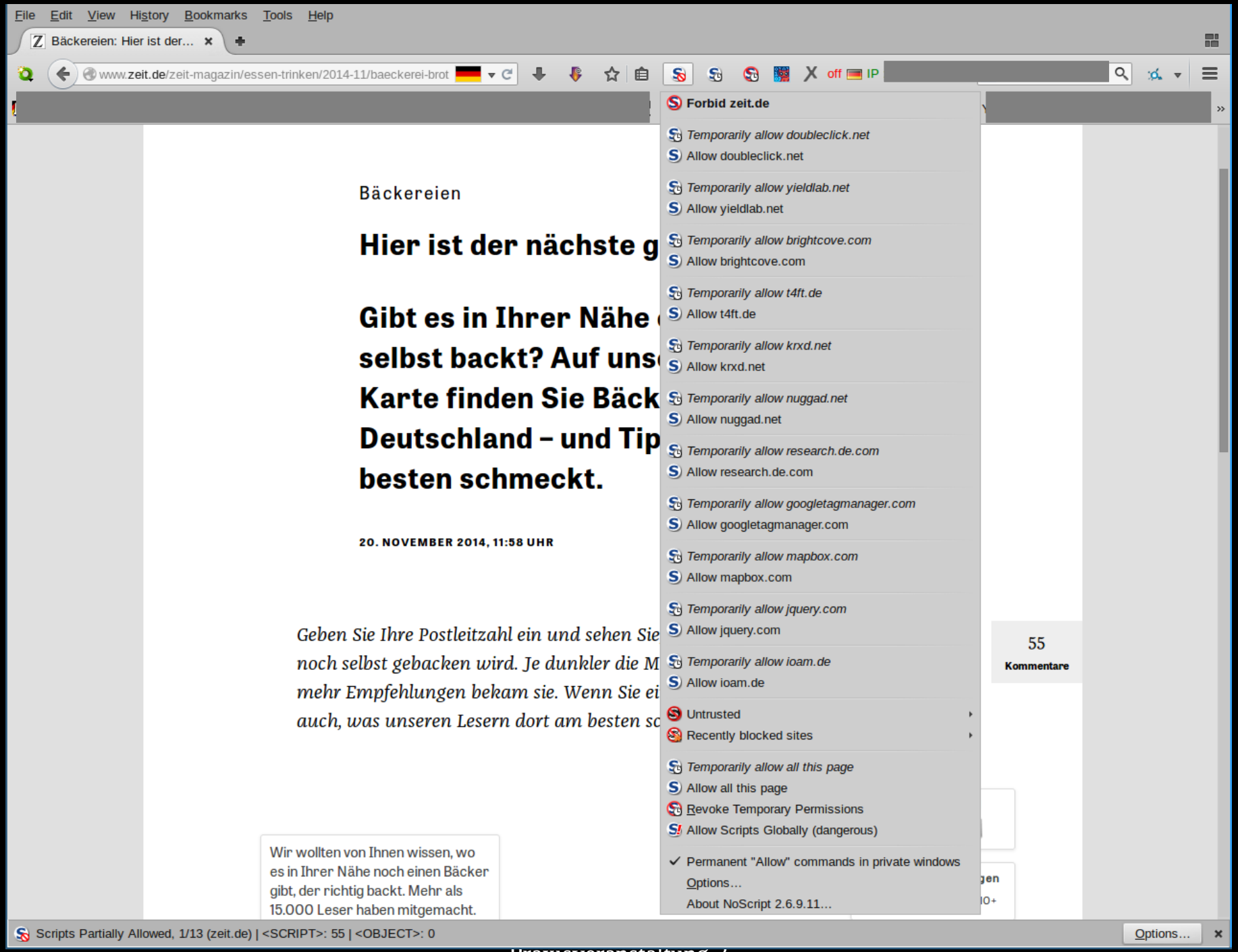
→ „Bäckereikarte“ von zeit.de

Theorieteil 2/4 - NoScript



Bildnachweis: Bildschirmfoto (Roland Hummel).

Theorieteil 2/4 - NoScript



Bildnachweis: Bildschirmfoto (Roland Hummel).

Theorieteil 4/4 - TOR

1. Einführung und „Belehrung“

2. visible VS invisible Web

→ Surface Web, Darknet, Deep Web

2. pro und contra

3. Anwendungsmöglichkeiten

4. TOR Browser Bundle

5. IP-Vergleich

6. eine .onion-Seite finden

7. eine .onion-Seite abrufen

Pause

10min

Praxisteil 1/3

Do**I**t**Y**ourself

- einzeln oder in Gruppen

- frei oder nach Aufgaben

Praxisteil 1/3 (Aufgaben)

1. Überprüfen Sie ihre **Passwörter** in Bezug auf Komplexität

→ http://www.passwordmeter.com/

2. Vergleichen Sie die Funktionalität ihrer favorisierten Webseiten per **Firefox und NoScript** ohne und mit deaktivierten Java Script-Funktionen – forschen Sie nach, welche Dienstleister sich hinter den blockierten Seiten verbergen!

→ http://www.focus.de/

3. Suchen Sie ihre favorisierten Webseiten über **YaCy** und nehmen Sie sie ggf. in Ihren Index auf, falls die Suche keine Ergebnisse liefert!

→ http://localhost:8090

4. Vergleichen Sie ihre **IP-Adresse** mittels http://myip.is/ mit und ohne TOR-Browser und besuchen Sie ihre favorisierten Webseiten über den **TOR-Browser** (vorinstalliert auf ihrem Desktop)!

5. Auf eigene Verantwortung: Machen Sie eine Exkursion ins **Deep Web** mit dem TOR-Browser!
Kleine Starthile: https://de.wikipedia.org/wiki/The_Hidden_Wiki

6. Probieren Sie weitere Add-ons aus:

→ Adblock Edge – anonymoX – CanvasBlocker – Flagfox – HTTPS-Everywhere (nicht direkt unter Add-ons) – Self-Destructing Cookies - WOT

Praxisteil 2/3

Reflexion

Praxisteil 3/3

Empfehlung:
https://myshadow.org/

Abschluss

1. für **Rechtfertigungssituation** Trilemma als Argumentationsgrundlage:

→ komfortabel?

→ kostenlos?

→ datenschonend/sicher?

-> max. zwei Eigenschaften bekommt man

2. **Vorbild** im Umgang mit digitalen Medien sein

3. **Konsequenz** auch in unbequemen Situationen

4. Weiterbilden (geht auch unkompliziert(er) z.B. mit **sempervideo.de**)

5. Bitte um **Kritik** und ggf. **Empfehlung**